KAJIAN MANAJEMEN RISIKO PADA OTENTIKASI PESAN YANG MENGGUNAKAN *DIGITAL SIGNATURE* KRIPTOGRAFI HILL *CIPHER*

TESIS

Disusun sebagai salah satu syarat untuk
memperoleh gelar Magister Komputer
dari Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI

Oleh:

WAFIQAH YASMIN AZHAR

NPM: 2016210038

PROGRAM STUDI PASCASARJANA
MAGISTER SISTEM INFORMASI
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER LIKMI
BANDUNG
2018

KAJIAN MANAJEMEN RISIKO PADA OTENTIKASI PESAN YANG MENGGUNAKAN *DIGITAL SIGNATURE* KRIPTOGRAFI HILL *CIPHER*

Oleh:

WAFIQAH YASMIN AZHAR

NPM: 2016210038

Bandung, 26 Maret 2018

Menyetujui,

Dr. Djajasukma Tjahjadi, S.E., M.T.

Pembimbing

PROGRAM STUDI PASCASARJANA
MAGISTER SISTEM INFORMASI
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER LIKMI
BANDUNG

2018

Dipersembahkan untuk keluarga tersayang
Endang, Juli, dan Faris
Serta kekasih tercinta

ABSTRAK

KAJIAN MANAJEMEN RESIKO PADA OTENTIKASI PESAN YANG MENGGUNAKAN *DIGITAL SIGNATURE* KRIPTOGRAFI HILL *CIPHER*

Oleh:

WAFIQAH YASMIN AZHAR

NPM: 2016210038

Pertukaran informasi secara *digital* diperlukan guna mempermudah dan mempercepat proses pengiriman pesan. Namun tidak aja jaminan bahwa pesan yang dikirim selalu dalam keadaan aman. Diperlukan teknik otentikasi untuk menjamin apakah pesan tersebut dalam keadaan asli atau sudah mengalami perubahan. Oleh karena itu dibutuhkan penanda pada sebuah pesan seperti tanda tangan yang dikenal dengan teknik *digital signature.* Hill *Cipher* merupakan salah satu teknik *digital signature* yang sudah diimplementasikan untuk beberapa aplikasi, namun belum sepenuhnya ideal dalam memenuhi keamanan sebuah pesan karena adanya kerentanan-kerentanan yang terdapat pada Hill *Cipher*. Untuk mengurangi atau bahkan menghilangkan risiko dari kerentanan-kerentanan Hill *Cipher,* perlu dilakukan identifikasi risiko dengan menggunakan metodologi *risk management* yang terdapat pada NIST 800-30 yang disebut dengan teknik *risk assessment.*

Saat ini teknik yang menyerang kerentanan Hill *Cipher* adalah teknik kriptanalisis dengan analisis matematika. Namun teknik-teknik kriptanalisis tersebut belum dikaji menggunakan suatu metodologi dari *risk management*, sehingga kerentanannya belum dapat terukur serta upaya pencegahannya tiap tingkat kerentanan belum ditemukan secara terstruktur.

Dengan melakukan *risk assessment* berdasarkan metodologi yang terdapat pada NIST 800-30, risiko dari kerentanan Hill *Cipher* dapat dikurangi atau bahkan dihilangkan. Hasil dari proses *risk assessment* tersebut menghasilkan kontrol rekomendasi tiap kerentanan untuk meminimalisir akibat dari risiko kerentanan yang terdapat pada Hill *Cipher*.

Kata Kunci : *Digital Signature*, Hill *Cipher*, NIST 800-30, *Risk Assessment*

ABSTRACT

RISK MANAGEMENT STUDY ON A MESSAGING AUTHORATION USING DIGITAL SIGNATURE CRYPTOGRAPHY HILL CIPHER

By:

WAFIQAH YASMIN AZHAR

NPM: 2016210038

Digital information exchange is required to simplify and speed up the messaging process. But it does not guarantee that the messages send are always safe. Authentication techniques are required to ensure that in the original or changed state. Therefore a marker is required on a message such as a signature known as a digital signature technique. Hill Cipher is one of the digital signature techniques that have been implemented for some applications, but not yet fully ideal in meeting the security of a message because of the vulnerabilities contained in Hill Cipher. To reduce or even eliminate the risk of Hill Cipher vulnerabilities, risk identification is required using the risk management methodology of NIST 800-30, which is called risk assessment technique.

Currently the technique that attacks Hill Cipher vulnerability is a cryptanalysis technique with mathematical analysis. However, these cryptanalysis techniques have not been studied using a methodology of risk management, so that vulnerability can not be measured and prevention efforts of each level of vulnerability have not been found in a structured manner.

With risk assessment based on the methodologies in NIST 800-30, the risk of Hill Cipher vulnerability can be reduced or even eliminated. The results of the risk assessment process resulted in the recommendation control of each vulnerability to minimize the consequences of vulnerability risk in Hill Cipher.

Keywords : *Digital Signature*, Hill *Cipher*, NIST 800-30, *Risk Assessment*

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan kepada Allah SWT, atas rahmat dan karunia-Nya penulis dapat menyusun laporan tesis ini yang berjudul **"Kajian Manajemen Resiko Pada Otentikasi Pesan Yang Menggunakan *Digital Signature* Kriptografi Hill *Cipher*"** yang disusun sebagai salah satu syarat memperoleh gelar Magister di STMIK LIKMI Bandung program studi Sistem Informasi.

Penulis menyadari dalam penyusunannya masih banyak kekurangan mengingat keterbatasan pengalaman yang penulis miliki. Saran dan kritik senantiasa penulis harapkan demi kebaikan penulis untuk kedepannya. Semoga laporan tesis ini dapat bermanfaat bagi banyak pihak.

Tidak lupa pula penulis ucapkan terima kasih kepada:

1. Bapak Ana Hadiana, Dr. Eng. selaku ketua program studi Sistem Informasi STMIK LIKMI Bandung sekaligus dosen penguji
2. Bapak Dr. Djajasukma Tjahjadi, S.E,.M.T selaku dosen pembimbing
3. Bapak Dhanny Setiawan, S. T., M. T selaku dosen penguji
4. Kedua Orang Tua penulis atas jasa-jasanya kepada penulis
5. Seluruh Dosen, Staf, dan Karyawan STMIK Likmi Bandung
6. Rekan-rekan pasca sarjana Sistem Informasi angkatan 2016 STMIK LIKMI Bandung, dan
7. Semua yang berperan dalam penyusunan laporan tesis yang tidak bisa penulis sebutkan satu persatu.

Bandung, Maret 2018

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pertukaran informasi secara *digital* diperlukan guna mempermudah dan mempercepat proses pengiriman pesan. Namun tidak aja jaminan bahwa pesan yang kita kirim selalu dalam keadaan aman. Diperlukan teknik otentikasi untuk menjamin apakah pesan tersebut dalam keadaan asli atau sudah mengalami perubahan, terlebih jika informasi yang disampaikan tersebut bersifat penting dan rahasia. Perubahan-perubahan tersebut bisa saja terjadi karena beberapa faktor (Stalling, 1995). Pertama, ketika proses pertukaran informasi berlangsung pesan tersebut terpotong sehingga mengakibatkan *crash* atau tidak utuh. Kedua, informasi tersebut disadap oleh seseorang yang tidak seharusnya mempunyai hak akses. Ketiga, adanya perubahan isi pesan oleh orang yang tidak mempunyai hak akses. Keempat, pesan tersebut digantikan dengan pesan palsu oleh orang yang tidak mempunyai hak akses. Oleh karena itu dibutuhkan penanda pada sebuah pesan seperti tanda tangan *digital* yang digunakan untuk otentikasi keaslian suatu pesan dari pengirim kepada si penerima pesan. Teknik tersebut dalam ilmu kriptologi dikenal dengan istilah teknik *digital signature.*

Salah satu teknik *digital signature* yang diketahui adalah teknik *digital signature* dengan algoritme kriptografi Hill *Cipher*. Hill *Cipher* menggunakan kunci simetris berupa matriks untuk proses enkripsi dan dekripsinya sebagai otentikasi pada suatu pesan. Saat ini teknik *digital signature* kriptografi Hill *Cipher* telah diimplementasikan untuk beberapa aplikasi, seperti enkripsi data pada *Short Messege Service* (SMS) berbasis Android (Cahyono, 2014) dan enkripsi pada *database* inventaris pertokoan (Santosa, 2013). Pada implementasinya teknik *digital signature* kriptografi Hill *Cipher* belum sepenuhnya ideal dalam memenuhi keamanan sebuah pesan karena adanya kerentanan-kerentanan yang terdapat pada penggunaan kunci Hill *Cipher*. Kerentanan-kerentanan tersebut dapat berpotensi untuk merusak integritas serta kerahasiaan pesan sebagai teknik otentikasi suatu pesan.

Untuk mengurangi atau bahkan menghilangkan risiko dari kerentanan-kerentanan Hill *Cipher,* perlu dilakukan identifikasi risiko dalam penggunaan *digital signature* kriptografi Hill *Cipher.* Teknik identifikasi risiko dan dampak serta upaya pencegahannya dalam metodologi *risk management* yang terdapat pada NIST 800-30 disebut dengan teknik *risk assessment* (Stoneburner., dkk. 2002).

Risk assessment penting dilakukan untuk menentukan kemungkinan sumber ancaman yang memanfaatkan kerentanan atau kelemahan dari *digital signature* kriptografi Hill *Cipher.* Teknik kriptanalisis merupakan salah satu ancaman yang menyerang kerentanan Hill *Cipher*. Teknik kriptanalisis pada Hill *Cipher* yang diketahui adalah dengan analisis matematika menggunakan persamaan linier, perkalian matriks (Munir, 2006), dan determinan matriks (Azhar., dkk. 2017). Namun teknik kriptanalisis tersebut belum dikaji menggunakan suatu metodologi dari *risk management*, sehingga analisis Hill *Cipher* terhadap serangan kriptanalisis belum dapat terukur kerentanannya serta upaya pencegahannya tiap tingkat kerentanan belum ditemukan secara terstruktur.

NIST *(National Institute of Standards and Technology)* 800-30 merupakan panduan manajemen risiko untuk sistem teknologi informasi yang ditulis oleh Gary Stoneburner, Alice Goguen, dan Alexis Feringa tahun 2002 yang direkomendasikan dari Institut Nasional Standar dan Teknologi. NIST 800-30 merupakan sebuah panduan yang memberikan dasar bagi pengembang program untuk memanajemen risiko yang efektif sebagai panduan praktis yang diperlukan untuk menilai dan mengurangi risiko yang diidentfikasi dalam sistem TI. Tujuan utama dari NIST 800-30 adalah membantu suatu organisasi untuk mengelola risiko misi terkait TI dengan lebih baik.

Oleh karena itu dalam penelitian ini penulis akan melakukan *risk assessment* berdasarkan metodologi yang terdapat pada NIST 800-30 terhadap pesan yang sudah ditandatangani menggunakan *digital signature* kriptografi Hill *Cipher* yang diharapkan dapat mengurangi atau bahkan menghilangkan risiko akibat kerentanan yang terdapat pada Hill *Cipher* dengan tema “Kajian Manajemen Resiko Pada Otentikasi Pesan Yang Menggunakan *Digital Signature* Kriptografi Hill *Cipher*”.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang diuraikan, maka rumusan masalah dalam penelitian ini adalah :

1. Apakah dengan melakukan *risk assessment* menggunakan NIST 800-30 dapat mengurangi dampak akibat keren
2. tanan yang terdapat pada Hill *Cipher*?
3. Bagaimana upaya *risk assessment* yang dilakukan untuk mengurangi dampak akibat kerentanan pesan yang sudah diotentikasi menggunakan *digital signature* kriptografi Hill *Cipher*?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah diuraikan sebelumnya, maka tujuan dalam penelitian ini adalah :

1. Untuk melakukan *risk assessment* menggunakan NIST 800-30 dalam mengurangi dampak akibat kerentanan yang terdapat pada Hill *Cipher*.
2. Menentukan upaya *risk assessment* yang dilakukan untuk mengurangi dampak akibat kerentanan terhadap pesan yang sudah diotentikasi menggunakan *digital signature* kriptografi Hill *Cipher*.

1.4 Ruang Lingkup Penelitian

Mengingat luasnya ruang lingkup penelitian, maka penulis membatasi permasalahan tersebut pada :

1. Teknik *digital signature* yang digunakan untuk otentikasi pesan adalah teknik kriptografi Hill *Cipher*.
2. Kerentanan Hill *Cipher* yang dianalisis adalah berdasarkan ketersediaan data dan kunci matriks Hill *Cipher*.
3. Teknik *risk assessment* yang digunakan adalah teknik *risk assessment* berdasarkan NIST 800-30.

1.5 Manfaat Penelitian

Adapun manfaat dari penelitian ini dilihat dari beberapa segi, yaitu:

1. Bidang Disiplin Ilmu Sistem Informasi

Dapat melakukan *risk assessment* pada pesan yang sudah ditandatangani oleh *digital signature* kriptografi Hill *Cipher* terhadap kerentannya menggunakan NIST 800-30 (Stoneburner., dkk. 2002).

2. Dunia Pendidikan

Menambah referensi penelitian dalam dunia pendidikan dalam bidang manajemen risiko yang dapat dijadikan pembelajaran untuk penelitian selanjutnya.

3. Masyarakat

Risk assessment pada pesan yang sudah ditandatangani oleh *digital signature* kriptografi Hill *Cipher* menggunakan NIST 800-30 (Stoneburner., dkk. 2002) dapat diterapkan di lingkungan masyarakat apabila diperlukan.

4. STMIK Likmi Bandung

Menjadi sarana evaluasi bagi pihak pengelola STMIK Likmi Bandung untuk mengetahui sejauh mana kualitas ilmu dan keterampilan yang selama ini telah diberikan kepada para mahasiswa.

5. Penulis

Sarana bagi penulis untuk pengimplementasian teknik *risk assessment* pada pesan yang sudah ditandatangani oleh *digital signature* kriptografi Hill *Cipher* terhadap kerentanannya menggunakan NIST 800-30 (Stoneburner., dkk. 2002) sebagai pembuktian metodologi dari *risk management*.

1.6 Sistematika Penulisan

Tesis ini disusun menjadi lima bab dengan sistematika sebagai berikut :

BAB I PENDAHULUAN

Bab satu menjelaskan latar belakang mengenai otentikasi pesan, faktor-faktor yang menyebabkan perubahan pada suatu pesan, *digital signature* dengan kriptografi Hill *Cipher* serta penerapannya, kriptanalisis*,* teknik *risk assessment* pada *digital signature.* Rumusan masalah bagaimana upaya *risk assessment* terhadap kerentanan Hill *Cipher*. Tujuan penelitian dilakukannya *risk assessment* pada *digital signature* kriptografi Hill *Cipher*. Ruang lingkup penelitian mengenai teknik *digital signature* dan jenis kerentanan Hill *Cipher*, serta sistematika penulisan.

BAB II LANDASAN TEORI

Bab dua menjelaskan tentang uraian dari judul tesis mengenai *Entity Authentication, Information Security Objective,* Tanda Tangan, *Digital Signature,* Kriptografi, Kriptografi Hill *Cipher*, *Security Attack Model, Cryptanalysis,* dan *Risk Assessment.*

BAB III METODE PENELITIAN

Bab tiga menjelaskan metode penelitian yang dilakukan, apa saja yang harus dipersiapkan dan dilakukan pada saat melakukan *risk assessment* pada *digital signature* kriptografi Hill *Cipher* terhadap kerentanannya*.*

BAB IV HASIL DAN PEMBAHASAN

Bab empat membahas mengenai hasil yang didapatkan setelah melakukan tahapan-tahapan *risk assessment* pada *digital signature* kriptografi Hill *Cipher* terhadap kerentanannya sesuai dengan metode penelitian yang sudah dilakukan.

BAB V KESIMPULAN DAN SARAN

Bab lima berisi kesimpulan dari seluruh hasil penelitian dan saran dari penulis berkaitan dengan hasil *risk assessment* pada *digital signature* kriptografi Hill *Cipher* untuk otentikasi suatu pesan terhadap kerentanannya.

BAB II
LANDASAN TEORI

2.1 *Entity Authentication* (Otentikasi Entitas)

Otentikasi entitas adalah proses dimana satu pihak diyakinkan (melalui akuisisi bukti yang menguatkan) tentang identitas pihak kedua yang terlibat dalam sebuah protokol, dan pihak kedua benar-benar berpartisipasi (yaitu aktif pada atau sebelum bukti diperoleh) (Menezes., dkk. 1996). Faktor-faktor yang bisa diidentifikasi adalah:

1. *Something known* (sesuatu yang diketahui), contohnya seperti *password*, *Personal Identification Number* (PIN), dan kunci rahasia pribadi.
2. *Something possessed* (sesuatu yang dimiliki), yaitu sesuatu yang berwujud fisik seperti paspor, kartu magnetik, kartu chip, dan *smart card.*
3. *Something inherent* (sesuatu yang ada pada diri manusia), yaitu sesuatu yang ada pada diri manusia (biometrik) seperti tanda tangan, sidik jari, suara, pola retina, dan garis tangan.

2.2 *Information Security* Objectives (Tujuan Keamanan Informasi)

Tujuan keamanan informasi menurut Menezes., dkk (1996) adalah:

1. *Confidentiality* (kerahasiaan pesan), yaitu kriptografi menjaga kerahasiaan pesan dengan cara mengenkripsinya ke dalam bentuk yang tidak mempunyai makna.
2. *Data integrity* (keaslian pesan), hal ini berkaitan dengan keutuhan (*integrity*) pesan. Dengan kata lain, hal ini dapat diungkapkan sebagai pertanyaan: “Apakah pesan yang diterima tidak mengalami perubahan (modifikasi)?”
3. *Authentication* (keabsahan), Hal ini berkaitan dengan kebenaran identitas pengirim. Dengan kata lain, hal ini dapat diungkapkan sebagai pertanyaan: “Apakah pesan yang diterima benar-benar berasal dari pengirim yang sesungguhnya?”
4. *Non-repudiation* (anti penyangkalan), yaitu pengirim tidak dapat menyangkal (berbohong) tentang isi pesan yang dikirim.

2.3 Tanda Tangan

Sejak berabad-abad lamanya, tanda tangan digunakan untuk membuktikan otentikasi dokumen kertas (misalnya surat, piagam, ijazah, buku, karya seni, dan sebagainya). Tanda tangan mempunyai karakteristik sebagai berikut (Munir, 2004):

1. Tanda tangan adalah bukti yang otentik
2. Tanda tangan tidak dapat dilupakan
3. Tanda tangan tidak dapat dipindah untuk digunakan ulang
4. Dokumen yang telah ditandatangani tidak dapat diubah
5. Tanda tangan tidak dapat disangkal

2.4 *Digital Signature* (Tanda Tangan *Digital*)

Fungsi tanda tangan pada dokumen kertas juga diterapkan untuk otentikasi pada data *digital* seperti pesan yang dikirim melalui saluran komunikasi dan dokumen elektronis yang disimpan didalam memori komputer. Tanda tangan pada data *digital* ini disebut tanda tangan *digital (digital signature)*. Yang dimaksud dengan tanda tangan *digital* bukanlah tanda tangan yang di-digitisasi dengan alat *scanner,* tetapi suatu nilai kriptografis yang bergantung pada pesan dan pengirim pesan (Hal ini kontras dengan tanda tangan pada dokumen kertas yang bergantung hanya pada pengirim dan selalu sama untuk semua dokumen). Dengan tanda tangan *digital*, maka integritas data dapat dijamin, disamping itu *digital signature* juga digunakan untuk membuktikan asal pesan (keabsahan pengirim), dan anti-penyangkalan (Munir, 2004).

Berikut merupakan beberapa pengertian mengenai *digital signature (*Menezes., dkk. 1996) :

1. Tanda tangan *digital* adalah string data yang menghubungkan pesan (dalam bentuk *digital*) dengan beberapa entitas asal.
2. Algoritma tanda tangan *digital* (atau algoritma tanda tangan) adalah metode untuk menghasilkan tanda tangan *digital*.
3. Algoritma verifikasi tanda tangan *digital* (atau algoritma verifikasi) adalah metode untuk memverifikasi bahwa tanda tangan *digital* itu asli (yaitu, memang dibuat oleh entitas yang ditentukan).
4. Proses penandatanganan tanda tangan *digital* (atau prosedur) terdiri dari algoritma tanda tangan *digital* (matematis), bersama dengan metode untuk memformat data menjadi pesan yang dapat ditandatangani.

2.4.1 Cara Menandatangani Pesan

Menandatangani pesan dapat dilakukan dengan dua cara (Munir, 2004) :

1. Penandatangan dengan Cara Mengenkripsi Pesan
   a. Menandatangani Pesan dengan Algoritma Simetri

      Pesan yang dienkripsi dengan algoritma simetri sudah memberikan solusi untuk otentikasi pengirim dan keaslian pesan, karena kunci simetri hanya diketahui oleh pengirim dan penerima. Jadi, jika B menerima pesan dari A, maka B percaya pesan itu dari A dan isinya tidak mengalami perubahan, karena tidak ada orang lain yang mengetahui kunci selain A dan B.

      Namun, algoritma simetri tidak dapat menyediakan suatu mekanisme untuk mengatasi masalah penyangkalan, yaitu jika salah satu dari dua pihak, A dan B, membantah isi pesan atau telah mengirim pesan. Agar dapat mengatasi masalah penyangkalan, maka diperlukan pihak ketiga yang dipercaya oleh pengirim/penerima. Pihak ketiga ini disebut penengah (arbitrase).

b. Menandatangani Pesan dengan Algoritma Kunci-Publik

Jika algoritma kunci-publik digunakan, maka enkripsi pesan dengan kunci publik tidak dapat digunakan untuk otentikasi, karena setiap orang potensial mengetahui kunci-publik. Tetapi, jika enkripsi pesan menggunakan kunci privat si pengirim dan dekripsi pesan juga menggunakan kunci-publik si pengirim, maka kerahasiaan pesan (secrecy) dan otentikasi keduanya dicapai sekaligus. Ide ini ditemukan oleh Diffie dan Hellman.

2. Tanda Tangan dengan Menggunakan Fungsi *Hash*

Penandanganan pesan dengan cara mengenkripsinya selalu memberikan dua fungsi berbeda: kerahasiaan pesan dan otentikasi pesan. Pada beberapa kasus, seringkali otentikasi yang diperlukan, tetapi kerahasiaan pesan tidak. Maksudnya, pesan tidak perlu dienkripsikan, sebab yang dibutuhkan hanya keotentikan pesan saja. Hanya sistem kriptografi kunci-publik yang cocok dan alami untuk pemberian tanda tangan *digital* dengan menggunakan fungsi *hash*. Hal ini disebabkan karena skema tanda tangan *digital* berbasis sistem kunci-publik dapat menyelesaikan masalah *non-repudiation* (baik penerima dan pengirim pesan mempunyai pasangan kunci masing-masing).

2.4.2 Proses Pemberian Tanda Tangan *Digital* (*Signing*)

Proses pemberian tanda tangan *digital* dapat dilakukan dengan cara berikut :

1. Pesan yang hendak dikirim diubah terlebih dahulu menjadi bentuk yang ringkas yang disebut *message digest. Message digest* (MD) diperoleh dengan mentransformasikan pesan M dengan menggunakan fungsi *hash* satu arah *(one way)* H,

2. MD = H(M)

3. Pesan yang sudah diubah menjadi *message digest* oleh fungsi *hash* tidak dapat dikembalikan lagi menjadi bentuk semula walaupun digunakan algoritma dan kunci yang sama (itulah sebabnya dinamakan fungsi *hash* satu arah).
4. Sembarang pesan yang berukuran apapun diubah oleh fungsi *hash* menjadi

message digest yang berukuran tetap. *Message digest* disebut juga nilai *hash (hash value)* dari fungsi *hash*, H.

5. Selanjutnya, *message digest* MD dienkripsikan dengan algoritma kunci-publik menggunakan kunci privat (SK) pengirim menjadi tanda tangan *digital* S,

   6. S = ESK(MD)

7. Pesan M disambung (append) dengan tanda tangan *digital* S, lalu keduanya dikirim melalui saluran komunikasi. Dalam hal ini, kita katakan bahwa pesan M sudah ditandatangani oleh pengirim dengan tanda tangan *digital* S.
8. Di tempat penerima, tanda tangan diverifikasi untuk dibuktikan keotentikannya dengan cara berikut:
   a. Tanda tangan *digital* S didekripsi dengan menggunakan kunci publik (PK) pengirim pesan, menghasilkan *message digest* semula, MD, sebagai berikut:

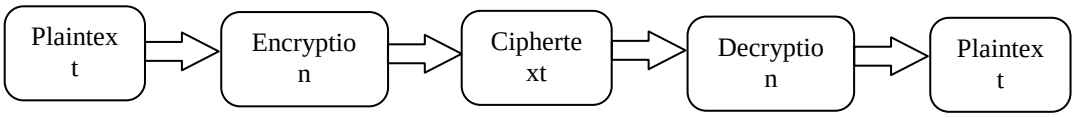
      MD = DPK(S)

   b. Pengirim kemudian mengubah pesan M menjadi *message digest* MD' menggunakan fungsi *hash* satu arah yang sama dengan fungsi *hash* yang digunakan oleh pengirim.
   c. Jika MD' = MD, berarti tanda tangan yang diterima otentik dan berasal dari pengirim yang benar.

2.5 Kriptografi

Data yang bisa dibaca dan dipahami tanpa langkah-langkah khusus yang disebut *plaintext* atau *cleartext*. Metode menyamarkan *plaintext* sedemikian rupa untuk menyembunyikan substansinya disebut enkripsi. Hasil enkripsi *plaintext* menjadi sesuatu yang tidak dapat terbaca disebut *ciphertext*. Proses mengembalikan *ciphertext* ke *plaintext* aslinya disebut dekripsi (NA, 1999).

Kriptografi merupakan ilmu mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Proses enkripsi dilakukan menggunakan suatu algoritme dengan beberapa parameter. Biasanya algoritme tidak dirahasiakan, bahkan enkripsi yang mengandalkan kerahasiaan algoritme dianggap sesuatu yang tidak baik. Rahasia terletak di beberapa parameter yang digunakan, jadi kunci ditentukan oleh parameter. Parameter yang menentukan kunci dekripsi itulah yang harus dirahasiakan (Kromodimoeljo, 2009).



Gambar 2.1
Proses Enkripsi dan Dekripsi (NA, 1999)

2.6 Kriptografi Hill *Cipher*

Hill *Cipher* diciptakan oleh Lester S. Hill pada tahun 1929. Hill *Cipher* menggunakan operasi aljabar linear matriks n x n untuk mengenkripsi dan dekripsi pesannya. Untuk mengenkripsi pesan dengan Hill *Cipher* dimulai dengan menetapkan angka antara 0 hingga 25 setiap huruf pada alfabet. Seperti yang ditunjukan oleh tabel berikut (Worthington, 2010) :

Tabel 2.1
Substitusi Huruf dan Nomor

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Hill *Cipher* dapat menggunakan matriks A berukuran 2 x 2 untuk mengenkripsi

datanya, sedangkan untuk dekripsinya dapat menggunakan matriks B yang *invertible* sesuai dengan matriks pada saat proses enkripsi (Worthington, 2010), seperti :

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Bentuk invers matriks B adalah :

$$B = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

2.6.1 Enkripsi Kriptografi Hill *Cipher*

Untuk melakukan enkripsi gunakan matriks A.

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

Langkah-langkah untuk melakukan enkripsinya adalah :

1. Bagi kata yang akan dienkripsi menjadi 2 blok huruf, kemudian substitusi kedalam bentuk angka.
2. Kalikan blok huruf yang telah disubstitusi kepada matriks A.
3. Hasil dari perkalian matriks moduluskan dengan 26.
4. Angka yang didapat dari hasil dari modulus 26 substitusikan kembali menjadi huruf.
5. Sehingga didapat hasil enkripsinya.

2.6.2 Dekripsi Kriptografi Hill *Cipher*

Untuk melakukan dekripsi gunakan matriks B.

$$B = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Langkah-langkah untuk melakukan dekripsinya adalah :

1. Bagi kata yang akan didekripsi menjadi 2 blok huruf, kemudian substitusi kedalam bentuk angka.
2. Kalikan blok huruf yang telah disubstitusi kepada matriks B.
3. Hasil dari perkalian matriks moduluskan dengan 26.
4. Angka yang didapat dari hasil dari modulus 26 substitusikan kembali menjadi huruf.
5. Sehingga didapat hasil dekripsinya.

2.7 *Security Attack Model* (Jenis Serangan Keamanan)

Menurut W. Stallings, "*Network & Internetwork Security*", Prentice Hall, 1995. penyerangan keamanan jaringan terdiri dari:

1. *Interruption* (Interupsi)

Interupsi adalah Pengerusakan informasi yang dikirimkan dalam jaringan, sehingga terpotong di tengah jalan dan gagal sampai ke tujuan. Serangan semacam ini menyerang ketersediaan suatu informasi ketika dibutuhkan (*availability*) suatu informasi. Contoh penyerangannya:

a. DOS yaitu serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (*resource*) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar.
b. DDOS yaitu jenis serangan *Denial of Service* (DOS) yang menggunakan banyak host (baik itu menggunakan komputer yang didedikasikan untuk melakukan penyerangan atau komputer yang "dipaksa" menjadi *zombie*) untuk menyerang satu buah *host* target dalam sebuah jaringan.

3. *Interception* (Pengalihan)

Pengalihan adalah seseorang yang tidak memiliki hak akses, bisa berupa user,

program, atau komputer, menyusup untuk mengakses sistem yang ada. Ini adalah serangan terhadap terhadap data yang sensitif (*confidentiality*) suatu jaringan. Contoh penyerangannya:

a. *Wiretapping* (penyadapan) yaitu suatu kejahatan yang berupa penyadapan saluran komunikasi khususnya jalur yang menggunakan kabel.
b. *Sniffing* yaitu penyadapan terhadap lalu lintas data pada suatu jaringan komputer.

4. *Modification* (Pengubahan)

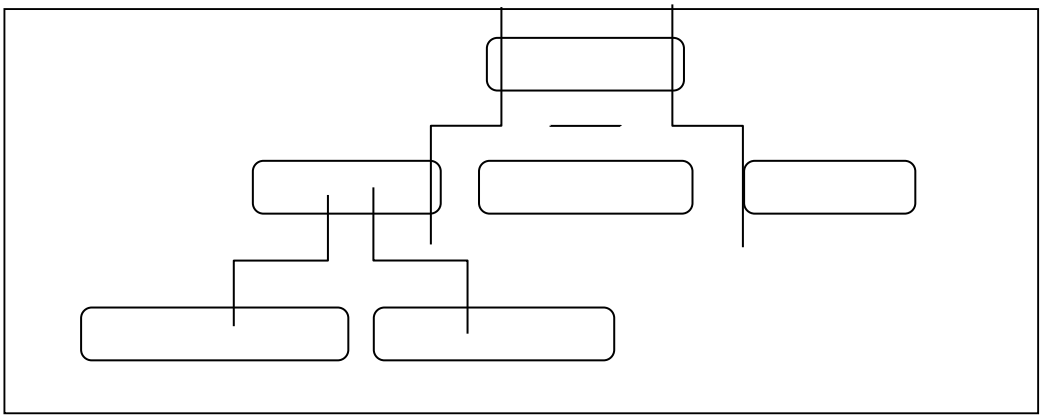
Pengubahan adalah pihak yang tidak memiliki hak akses, tidak hanya bisa menyusup ke sistem, dapat juga mengubah isi aset. Serangan semacam ini menyerang terhadap pengubahan (*integrity*) suatu informasi. Contoh penyerangannya:

a. Mengubah tampilan website (*defacing*), menempelkan Trojan (virus) pada web atau email, atau pemakai lain yang mengubah informasi tanpa izin.
b. *"Man in the middle attack"* dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain.

5. *Fabrication* (Pemalsuan)

Pemalsuan adalah seseorang yang tidak memiliki hak akses, memasukkan suatu objek palsu ke dalam sistem yang ada. Serangan ini menyerang keaslian (*authentication*) suatu informasi. Contoh penyerangannya seperti *phising mail* yaitu memasukkan pesan-pesan palsu seperti e-mail palsu ke dalam jaringan komputer.

2.8 *Cryptanalysis* (Kriptanalisis)



Gambar 2.2
Cryptanalysis (Paar dan Pelzi. 1998)

Kriptanalisis adalah ilmu dan (terkadang disebut seni) untuk memecahkan kriptosistem. Kriptanalisis sangat penting bagi kriptosistem modern karena tanpa kriptanalisis, kita tidak akan pernah tahu apakah metode kripto kita benar-benar aman atau tidak (Paar dan Pelzi. 1998). Kriptanalisis terbagi menjadi beberapa bagian (Paar dan Pelzi. 1998):

1. *Classical Cryptanalysis* (kriptanalisis klasik) adalah teknik untuk memulihkan *plaintext* x dari *ciphertext* y, atau mengembalikan kunci k dari *ciphertext* y.
    a. *Mathematic Analysis* (analisis matematika) yaitu teknik dengan menggunakan analisa matematika.
    b. *Brute Force Attack* (serangan *brute force*) yaitu teknik dengan menguji semua kunci yang mungkin menjadi kunci kriptologi tersebut.
2. *Implementation Attack* (serangan implementasi langsung) yaitu menyerang akses fisik seperti pada *smart card.*
3. *Social Engineering* (rekayasa sosial), yaitu seperti menyuap, memeras, menipu, atau spionase klasik lainnya untuk mendapatkan kunci melalui interaksi dengan manusia.

Kriptografi menyebabkan timbulnya kriptanalisis, yaitu ilmu pengetahuan dan seni untuk membongkar data acak. Praktisi dari kriptanalisis disebut kriptanalis. Setiap ada algoritme kriptografi baru yang dibuat oleh kriptografer langsung diikuti oleh adanya upaya percobaan kriptanalisis. Percobaan kriptanalisis ini disebut *attack* (serangan). Kriptanalisis mencoba mengembalikan data jelas tanpa menggunakan akses ke kunci kriptografi. Asumsi dasar dari suatu kriptosistem adalah bahwa seorang kriptanalis

mengetahui keseluruhan mekanisme enkripsi, terkecuali kuncinya. Berdasarkan hal itu maka serangan terhadap kriptografi diklasifikasikan menjadi empat, yaitu (Munir, 2006) :

1. *Ciphertext-only attack*

Pada jenis serangan ini, kriptanalis mempunyai *ciphertext* dari beberapa data yang dienkripsikan dengan algoritme kriptografi yang sama. Tujuan kriptanalis adalah mendapatkan *plaintext* dari *ciphertext* atau lebih baik lagi menarik kesimpulan mengenai kunci yang digunakan.

2. *Known-plaintext attack*

Pada jenis serangan ini, kriptanalis tidak hanya memiliki *ciphertext*, tetapi juga *plaintext* dari *ciphertext* tersebut. Tujuan kriptanalis adalah untuk menarik kesimpulan mengenai kunci yang digunakan untuk mengenkripsi data atau algoritme untuk mendekripsikan *ciphertext*.

3. *Chosen-plaintext attack*

Pada jenis serangan ini, kriptanalis selain mengetahui *ciphertext* dan *plaintext*, juga dapat memilih *plaintext* yang diinginkan yang biasanya memiliki lebih banyak informasi tentang kunci. Tujuan kriptanalis adalah menarik kesimpulan mengenai kunci yang digunakan untuk mengenkripsi data.

4. *Adaptive-chosen-plaintext attack*

Dalam hal ini kriptanalis tidak hanya dapat memilih *plaintext* yang telah dienkripsi, tetapi juga dapat memodifikasi pilihan tersebut berdasarkan hasil enkripsi sebelumnya. Kriptanalis mengetahui blok *plaintext* yang lebih kecil dan kemudian memilih yang lain berdasarkan hasil enkripsi pertama, kedua, dan seterusnya.

2.9 Kriptanalisis Hill *Cipher*

Teknik kriptanalisis pada Hill *Cipher* yang telah diketahui adalah teknik kriptanalisis mengunakan analisis matematika. Teknik analisis matematika tersebut menggunakan persamaan linier, perkalian matriks (Munir, 2006), dan determinan matriks (Azhar., dkk. 2017) untuk membobol suatu pesan. Teknik tersebut digunakan apabila potongan *plaintext*-nya diketahui minimal empat huruf, dan kunci Hill *Cipher* yang

digunakan adalah berordo 2 x 2. Berikut adalah langkah-langkah dari teknik analisis matematika mengunakan persamaan linier, perkalian matriks, dan determinan matriks.

2.9.1 Persamaan Linier

Langkah-langkah analisis matematika mengunakan persamaan linier adalah sebagai berikut (Munir, 2006):

1. Definisikan 4 huruf *plaintext* dan *ciphertext*
2. Representasikan kedalam bentuk matrix 2 x 2
3. Implementasikan kedalam rumus Hill *Cipher* **C = K . P**

Dimana C = *Ciphertext*, K = *Key*, P = *Plaintext*

Anggap Kunci : $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$

4. Subtitusi kedalam bentuk angka
5. Selanjutnya gunakan subtitusi persamaan pada matriks pada hasil dari C = K . P untuk mengetahui nilai dari masing-masing variabel kunci.
6. Kunci enkripsi ditemukan. Lakukan *inverse* untuk mengetahui kunci dekripsi.

2.9.2 Perkalian Matriks

Langkah-langkah analisis matematika mengunakan perkalian matriks adalah sebagai berikut (Munir, 2006):

1. Definisikan 4 huruf *plaintext* dan *ciphertext*
2. Representasikan kedalam bentuk matrix 2 x 2
3. Implementasikan kedalam rumus Hill *Cipher* **C = K . P**

Dimana C = *Ciphertext*, K = *Key*, P = *Plaintext*

Anggap Kunci : $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$

4. Subtitusi kedalam bentuk angka
5. Iimplementasikan kedalam rumus K = C . P^{-1}
6. Kunci enkripsi ditemukan. Lakukan *inverse* untuk mengetahui kunci dekripsi.

2.9.3 Determinan Matriks

Langkah-langkah analisis matematika mengunakan determinan matriks adalah sebagai berikut (Azhar., dkk. 2017):

1. Definisikan 4 huruf *plaintext* dan *ciphertext*
2. Representasikan kedalam bentuk matrix 2 x 2
3. Implementasikan kedalam rumus Hill *Cipher* **C = K . P**

Dimana C = *Ciphertext*, K = *Key*, P = *Plaintext*

anggap Kunci : $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$

4. Subtitusi kedalam bentuk angka
5. Ubah matriks kedalam bentuk aljabar linier
6. Cari Determinan Keseluruhan dan Determinan a, b, c, d

Catatan : “Determinan b” dan “Determinan d” **tidak ditukar posisi**

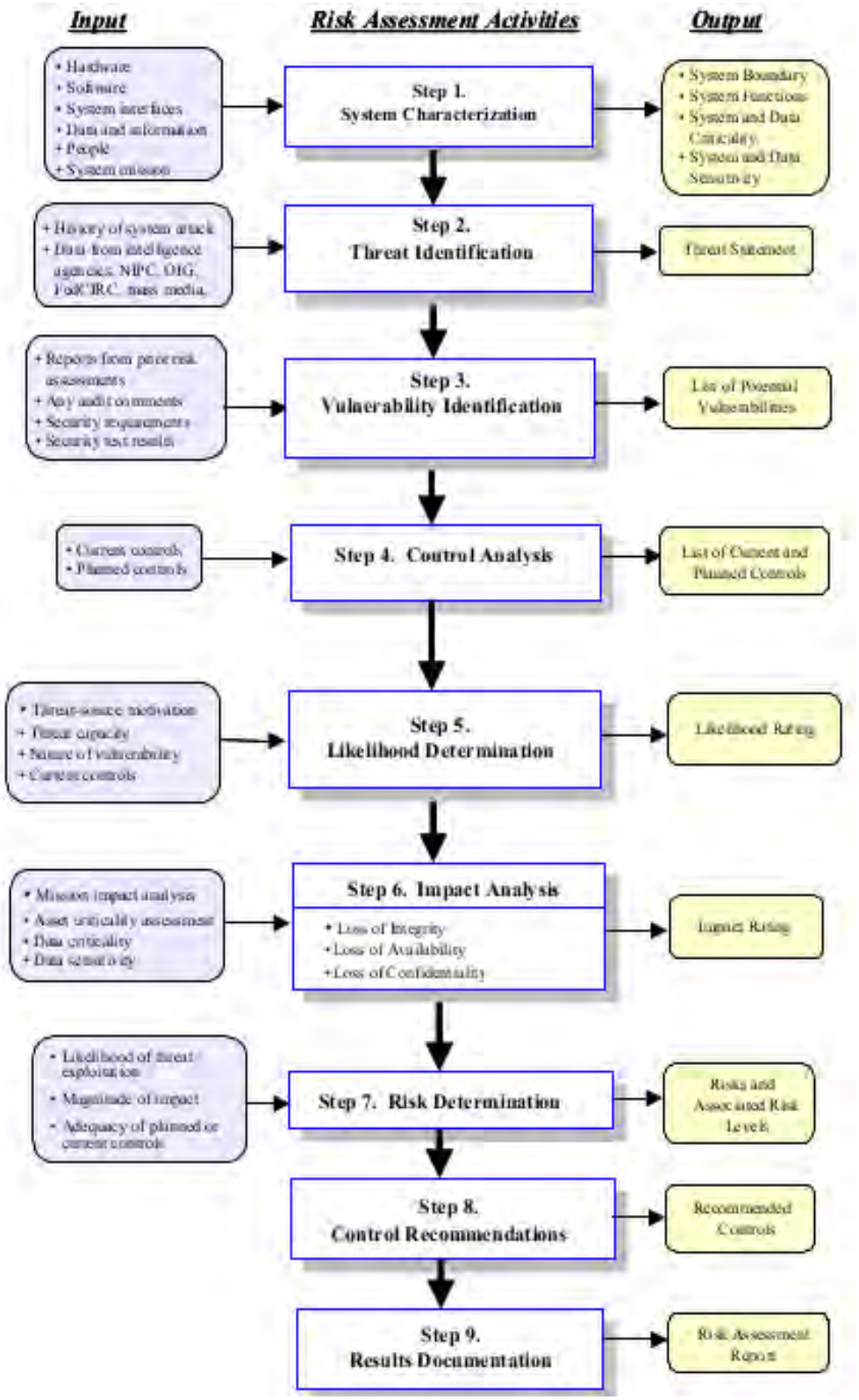
7. Det a, b, c, d dibagi dengan Det Keseluruhan
8. Kunci enkripsi ditemukan. Lakukan *inverse* untuk mengetahui kunci dekripsi.

2.10 *Risk Assessment* (Penilaian Risiko)

Penilaian risiko adalah proses pertama dalam metodologi manajemen risiko. Suatu organisasi menggunakan penilaian risiko untuk mengetahui tingkat ancaman potensial dan risiko yang terkait dengan sistem TI di seluruh SDLC-nya. Keluaran dari proses ini membantu mengidentifikasi pengendalian yang tepat untuk mengurangi atau menghilangkan risiko selama proses mitigasi risiko. Risiko adalah kemungkinan sumber

ancaman yang ada yang memanfaatkan potensi kerentanan tertentu, dan dampak yang dihasilkan dari kejadian buruk tersebut terhadap suatu organisasi. Untuk mengetahui kemungkinan terjadinya efek samping di masa depan, ancaman terhadap sistem TI harus dianalisis bersamaan dengan potensi kerentanan dan kontrol yang ada pada sistem TI. Metodologi penilaian risiko mencakup sembilan langkah yaitu (Stoneburner., dkk. 2002):

1. *Step 1 : System Characterization* (Karakterisasi Sistem)
2. *Step 2 : Threat Identification* (Identifikasi Ancaman)
3. *Step 3 : Vulnerability Identification* (Identifikasi Kerentanan)
4. *Step 4 : Control Analysis* (Analisis Kontrol)
5. *Step 5 : Likelihood Determination* (Kemungkinan Penentuan)
6. *Step 6 : Impact Analysis* (Analisis Dampak)
7. *Step 7 : Risk Determination* (Penentuan Risiko)
8. *Step 8 : Control Recommendations* (Rekomendasi Kontrol)
9. *Step 9 : Results Documentation* (Hasil Dokumentasi)



Gambar 2.3
Risk Assessment Methodology Flowchart
NIST 800-30 (Stoneburner., dkk. 2002)

2.10.1 *Step 1 : System Characterization* (Karakterisasi Sistem)

Langkah pertama adalah menentukan ruang lingkup. Pada tahap ini, batas-batas sistem TI diidentifikasi, bersama dengan sumber daya dan informasi yang membentuk sistem. Seperti perangkat keras, perangkat lunak, konektivitas sistem, dan divisi bertanggung jawab atau personil pendukung untuk menentukan risikonya.

Bagian 1 menjelaskan informasi terkait sistem yang digunakan untuk mengkarakterisasi sistem TI dan lingkungan operasionalnya. Bagian 2 menyarankan teknik pengumpulan informası yang dapat digunakan untuk mengumpuikan informasi yang relevan dengan lingkungan pemrosesan sistem TI. Metodologi yang dijelaskan dalam dokumen ini dapat diterapkan pada penlaian sistem tunggal atau multipel dan saling terkait.

1. Informasi Terkait Sistem

Mengidentfikasi risiko sistem TI memerlukan pemahaman yang tajam tentang lingkungan pemrosesan sistem. Orang yang melakukan peniliaian risiko harus mengumpulkan informasi yang berkaitan dengan sistem. dan biasanya diklasifikas kan sebagai berikut:

a. Perangkat keras
b. Perangkat lunak
c. Artarmuka sistem (seperti konektivitas internal dan eksternal)
d. Data dan informasi
e. Orang yang mendukung dan menggunakan sistem TI
f. Misi sistem (misalnya proses yang dilakukan oleh sitem TI)
g. Kekritisan sistem dan data (misainya nilai sistem atau kepentingan sebuah organisasi)
h. Sensitivitas sistem dan data

Informasi tambahan lainnya yang terkait adalah seperti:

a. Persyaratan fungsional sistem TI
b. Pengguna sistem (seperti pengguna sistem yang memberikan dukungan teknis ke sistem TI; pengguna aplikasi yang menggunakan sistem TI untuk menjalankan fungsi bisnis)
c. Kebjakan keamanan sistem yang mengatur sistem TI (kebijakan organisasi, persyaratan federal, hukum, praktik industri)
d. Arsitektur keamanan sistem
e. Topologi jaringan saat ini (seperti diagram jaringan)
f. Perlindungan penyimpanan informasi yang melindungi sistem dan ketersediaan data, integritas, dan kerahasiaan
g. Arus informasi yang berkaitan dengan sistem TI (misalnya, antarmuka sistem, diagram masukan sistem dan diagram alir output)
h. Kontrol teknis yang digunakan untuk sistem TI (seperti produk keamanan *buit-in* atau *add-on* yang mendukung identfkasi dan otentikasi, kontrol akses *discretionary* atau *mandatory*, audit, perlindungan informasi residual, metode enkripsi)
i. Kontrol manajemen yang digunakan untuk sistem TI (seperti peraturan perilaku perencanaan keamanan)
j. Kontrol operasional yang digunakan untuk sisterm TI (misalnya keamanan personil, cadangan, kontinjensi, dan operasi pemulhan dan pemeliharaan sistem, penyimpanan di luar lokasi, pembuatan akun pengguna dan prosedur penghapusan; kontrol untuk pemisahan fungsi pengguna, seperti pengguna istimewa akses versus akses pengguna standar)
k. Lingkungan keamanan fisik sistern TI (seperti keamanan fasilitas, pusat data kebijakan)
l. Keamanan lingkungan diterapkan untuk lingkungan pemrosesan sistem TI (seperti kontrol untuk kelembaban, air, listrik, polusi, suhu, dan bahan kimia).

Untuk sistem yang ada di tahap inisiasi atau perancangan, informasi sistem dapat diturunkan dari dokumen desain atau persyaratan. Untuk sistem TI yang sedang dikembangkan, perlu untuk mendefinisikan peraturan dan atribut keamanan kunci yang direncanakan untuk sistem TI masa depan. Dokumen disain sistem dan rencana keamanan sistem dapat membenkan informasi yang berguna tentang keamanan suatu sistem TI yang sedang dalam pengembangan. Untuk sistem TI operasional, data dikumpulkan mengenai sistem TI di lingkungan produksinya, termasuk data tentang konfigurasi sistem, konektivitas, dan prosedur dan praktik terdokumentasi dan tidak berdokumen. Oleh karena tu, deskripsi sistem dapat didasarkan pada keamanan yang diberikan oleh infrastruktur yang mendasarinya atau pada rencana keamanan masa depan untuk sistem TI.

2. Teknik Mengumpulkan Informasi

Setiap atau kombinasl dari teknik berikut dapat digunakan dalam mengumpulkan informasi yang relevan dengan sistem TI dalam batas operasionalnya, seperti:

a. Kuesioner. Untuk mengumpukan informasi yang relevan, personel penilaian risiko dapat mengembangkan kuesioner mengenai pengendalian manajemen dan operasional yang direncanakan atau digunakan untuk sistem TI. Kuesioner ini harus didistribusikan ke personil manajemen teknis dan nonteknis yang berlaku yang sedang merancang atau mendukung sistem TI. Kuesioner juga bisa digunakan selama kunjungan dan wawancara di tempat.
b. Wawancara di Tempat. Wawancara dengan personil dukungan sistem dan manajemen TI memungkinkan untuk mengumpulkan informasi bermanfaat tentang sistem TI (seperti bagaimana sistem dioperasikan dan dikelola). Kunjungan ke tempat juga memungkinkan untuk mengamati dan mengumpulkan informasi tentang keamanan fisik lingkungan, dan operasional sistem TI. Untuk sistem yang masih dalam tahap perancangan, kunjungan ke tempat adalah latihan mengumpulkan data tatap muka dan dapat memberi kesempatan untuk mengevaluasi lingkungan fisik dimana sistem TI akan beroperasi.

c. *Review* Dokumen. Dokumen kebjakan (misalnya dokumentasi legislatif, arahan), dokumentasi sistem (misainya panduan pengguna sistem, manual administrasi sistem, perancangan sistem dan dokumen persyaratan, dokumen akuisisi), dan dokumentasi terkait keamanan (misalnya laporan audit sebelurnnya, laporan penilaian risıko, sisterm hasil uji, rencana keamanan sistem, kebijakan keamanan) dapat memberikan informasi yang baik tentang kontrol keamanan yang digunakan dan direncanakan untuk sistem TI. Analisis dampak misi organisasi atau penilaian kekritisan aset membenkan informasi mengenai kekritisan dan sensitivitas sistem dan data.

d. Penggunasn Alat Pemindaian Otomatis. Metode teknis proaktif dapat digunakan untuk mengumpulkan informasi sistem secara efisien. Misalnya, alat pemetaan jaringan dapat mengidentfikasi layanan yang dijalankan pada sekelompok besar host dan menyediakan cara cepat untuk membangun profil individual dari sistem TI target.

Pengumpulan informasi dapat dilakukan selama proses penilaian risiko, mulai dari Langkah 1 (Karakterisasi Sistem) sampai dengan Langkah 9 (Dokumentasi Hasil).

Output dari Langkah 1 adalah penilaian karakterisasi sistem TI, gambaran yang baik tentang lingkungan sistem TI, dan penggambaran batas sistem.

2.10.2 *Step 2 : Threat Identification* (Identifikasi Ancaman)

Ancaman adalah potensi sumber ancaman tertentu untuk berhasil menerapkan kerentanan tertentu. Kerentanan adalah kelemahan yang secara tidak sengaja dipicu atau sengaja dieksploitasi. Sumber ancaman umum meliputi:

a. Ancaman alami seperti banjir, gempa bumi, tormado. tanah longsor, longsoran salju, badai listrik, dan kejadian lainnya.
b. Ancaman manusia seperti penstiwa yang dimungkinkan oleh atau disebabkan oleh manusia, seperti tindakan yang tidak disengaja (entri data yang tidak disengaja) ałau tindakan yang disengaja (serangan berbasis jaringan, upload perangkat lunak berbahaya, akses tidak sah ke informasi rahasia)
c. Ancaman lingkungan seperti kegagalan daya jangka panjang, polusi, bahan kimia, kebocoran calran.

Sumber ancaman tidak menimbulkan risiko bila tdak ada kerentanan yang bisa diserang. Dalam menentukan kemungkinan ancaman, seseorang harus mempertimbangkan sumber ancaman, potensi kerentanan, dan kontrol yang ada.

1. Identifikasi Sumber Ancaman

Tujuan dari langkah ini adalah untuk mengidentifikasi sumber ancaman potensial dan menyusun daftar pemyataan ancaman sumber ancaman potensial yang ada pada sistem TI yang sedang dievaluasi. Sumber ancarman didefiniskan sebagai keadan atau peristiwa yang berpotensi menyebabkan kerusakan pada sistem TI. Sumber-sumber ancaman yang umum bisa bersifat alami, manusiawi, atau lingkungan. Dalam menilai sumber ancaman, penting untuk mempertimbangkan semua yang dapat menyebabkan kerusakan pada sistem TI dan lingkungan pemrosesannya. Misalnya, ancaman untuk sistem TI yang berada di padang pasir mungkin tidak akan terkena dampak "banjir alami" karena tidak mungkiin terjadi. Ancaman yang mungkin terjadi yaitu seperti ledakan di ruang komputer dan menyebabkan kerusakan pada asel dan sumber daya Ti organisasi. Manusia bisa menjadi sumber ancaman melalui tindakan yang disengaja seperti yang dilakukan orang jahat atau karyawan yang tidak puas. Atau tindakan yang tidak

disengaja, seperti kelalaian dan kesalahan. Serangan yang disengaja dapat berupa (1) upaya jahat untuk mendapatkan akses tidak sah ke sistem TI (misalnya melalui tebakan kata kunci) untuk membahayakan sistem dan integritas data, ketersediaan, atau kerahasiaan atau (2) tujuan yang tidak berbahaya, namun tetap berusaha untuk menghindari keamanan sistem. Salah satu contoh jenis serangan yang disengaja adałah pemrogram menulis program kuda Trojan untuk memotong keamanan sistem.

2. Motivasi dan Tindakan Ancaman

Motivasi dan sumber daya untuk melakukan serangan membuat manusia berpotensi untuk menjadi sumber ancaman berbahaya. Tabel 2.2 menyajkan gambaran umum tentang banyak ancaman manusia dewasa ini, kemungkinan motivasi mereka, metode atau tindakan ancaman yang dilakukan. Informasi ini akan berguna bagi organisasi yang mempelajan lingkungan ancaman manusia mereka dan menyesuaikan pernyataan ancaman manusia mereka. Selain itu, ulasan sejarah, laporan pelanggaran keamanan, laporan kejadian, wawancara dengan administrator sistem, petugas bantuan, dan komunitas pengguna selama pengumpulan informasi akan membantu mengidentifikasi sumber ancaman manusia yang berpotensi membahayakan sistem TI dan datanya dan hal itu mungkin menjadi perhatian dimana adanya kerentanan.

Tabel 2.2
Ancaman Manusia: Sumber Ancaman, Motivasi, dan Tindakan Ancaman

Sumber Ancaman	Motivasi	Tindakan Ancaman
Hacker, cracker	Tantangan Ego Pemberontakan	Hacking Rekayasa sosial Sistem Intrusi, *break-in* Akses sistem yang tidak sah
Computer criminal	Pemusnahan informasi Pengungkapan informasi ilegal Keuntungan moneter Perubahan data yang tidak sah	Kejahatan komputer (seperti menguntit maya) Tindakan curang (peniruan/pemalsuan identitas, intersepsi) Penyuapan informasi Gangguan sistem
Terrorist	Pemerasan Penghancuran Eksploitasi Balas dendam	Bom/Terorisme Perang informasi Serangan sistem (seperti penolakan layanan pendistribusi) Penetrasi sistem Gangguan sistem

Sumber Ancaman	Motivasi	Tindakan Ancaman
Spionase industri (perusahaan, pemerintah asing, kepentingan pemerintah lainnya)	Keunggulan kompetitif Spionase ekonomi	Eksploitasi ekonomi Pencurian informasi Intrusi tentang privasi pribadi Rekayasa sosial Penetrasi sistem Akses sistem yang tidak sah (akses terhadap informasi rahasia, kepemilikan, dan teknologi)
Orang dalam (kurang terlatih, tidak puas, jahat, kelalaian, ketidakjujuran, atau karyawan yang dihentikan)	Rasa ingin tahu Ego Intelijen Keuntungan moneter Balas dendam Kesalahan dan kelalaian yang tidak disengaja (misalnya kesalahan entri data, kesalahan pemrograman)	Menyerang seorang karyawan Pemerasan Browsing kepemilikan informasi Penyalahgunaan komputer Penipuan dan pencurian Penyuapan informasi Memasukan data yang dipalsukan dan rusak Penangkapan Kode berbahaya (virus, trojan) Penjualan informasi pribadi Sistem bug Gangguan sistem Sistem Sabotase Akses sistem yang tidak sah

Pemyataan ancaman, atau daftar sumber ancaman potensial, harus disesuaikan dengan organisasi individual dan lingkungan pemrosesannya. Informasi tentang ancaman alam (misainya kebiasaan komputasi pengguna akhir). Secara umum, banjir, gempa bumi, badai) harus tersedia. Ancaman yang diketahui telah didentifkasi oleh banyak organisasi pemerintah dan sektor swasta. Alat deteksi intrusi juga menjadi lebih umum, dan organisasi pemerintah dan industri terus mengumpukan data tentang kejadian keamanan, sehingga meningkatkan kemampuan untuk meniai ancaman secara realistis. Sumber informasi tersebut bersumber darı:

1. Instansi intelijen (misalnya Pusat Pelindung Infrastruktur Nasional Biro Investigasi Federal)
2. Pusat Respon Insiden Komputer Federal (FedCIRC)
3. Media massa, terutama sumber daya berbasis Web seperti *SecurityFocus.com*, *SecurityWatch.com*, *SecurityPortal.com*, dan *SANS.org*

Output dari langkah 2 adalah sebuah pemyataan ancaman yang berisi daftar sumber ancaman yang dapat memanfaatkan kerentanan sistem.

2.10.3 *Step 3 : Vulnerability Identification (*Identifikasi Kerentanan*)*

Analisis ancaman terhadap sistem TI harus mencakup analisis kerentanan yang terkait dengan lingkungan sistem. Tujuan dari langkah ini adalah untuk mengembangkan daftar kerentanan sistem (kelemahan atau kelemahan) yang bisa dimanfaatkan oleh sumber ancaman potensial.

Kerentanan adalah kelemahan dalam prosedur keamanan sistem, perancangan, implementasi, atau pengendalian internal yang dapat dilakukan (tanpa sengaja dipicu atau sengaja dieksploitasi) dan mengakibatkan pelanggaran keamanan atau pelanggaran terhadap kebijakan keamanan sistem. Tabel 2.3 dibawah menampilkan contoh kerentanan terhadap ancaman.

Tabel 2.3
Kerentanan Terhadap Ancaman

Kerentanan	Motivasi	Tindakan Ancaman
Pengidentifikasi sistem karyawan yang dihentikan (ID) tidak dikeluarkan dari sistem.	Karyawan yang dihentikan	Mengakses data kepemilikan perusahaan
Firewall perusahaan memungkinkan inbound telnet, dan guest ID diaktifkan pada server xyz	Pengguna yang tidak berwenang (seperti peretas, karyawan yang dihentikan, penjahat komputer, teroris)	Menggunakan telnet ke server XYZ dan file sistem penjelajahan dengan ID tamu
Vendor telah mengidentifikasi kelemahan dalam perancangan keamanan sistem; Namun, patch baru belum diterapkan pada sistem.	Pengguna yang tidak berwenang (mis., Peretas, karyawan yang tidak puas, penjahat komputer, teroris)	Mendapatkan akses tidak sah ke file sistem sensitif berdasarkan kerentanan sistem yang diketahui
Pusat data menggunakan penyiram air untuk menekan api; terpal untuk melindungi perangkat keras dan peralatan dan kerusakan.	Api, orang lalai	Penyiam air diaktifkan di pusat data

Metode yang disarankan untuk mengidentrikasi kerentanan sistem adalah penggunaan sumber kerentanan, kinerja pengujian keamanan sistem, dan pengembangan daftar persyaratan keamanan. Perlu dicatat bahwa jenis kerentanan yang akan ada, dan metodologi yang diperlukan untuk menentukan apakah kerentanan ada, biasanya akan bervariasi tergantung pada sifat sistem TI dan fase yang di dalamnya, pada SDLC:

a. Jika sistem TI belum dirancang, pencarian kerentanan harus berfokus pada kebijakan keamanan organisasi prosedur keamanan yang direncanakan. Dan definisi persyaratan sistem, dan analisis produk keamanan vendor atau pengembang (misalnya dokumen putih).
b. Jika sistem TI sedang diterapkan, identifikasi kerentanan harus diperluas untuk mencakup informasi yang lebih spesifik, seperi fitur keamanan yang direncanakan yang dijelaskan dalam dokumentasi perancangan keamanan dan hasil uji dan evaluasi sistem sertfikasi.
c. Jika sistem TI beroperasi, proses identifikasi kerentanan hanus mencakup analisis terhadap fitur keamanan sistem TI dan kontrol keamanan, teknis dan prosedural, yang digunakan untuk melindungi sistem

1. Sumber Kerentanan

Kerentanan teknis dan nonteknis yang terkait dengan lingkungan pemrosesan sistem TI dapat didentifikasi melalui teknk pengumpulan infomasi. Tinjauan terhadap sumber industri lainnya (misal halaman Web vendor yang mengidentifikasi *bug* dan kekurangan sistem) akan berguna dalam mempersiapkan wawancara dan dalam mengembangkan kuesioner yang efektif untuk mengidentikasi kerentanan yang mungkin berlaku untuk sistem TI tertentu (misalnya versi spesifik dari sebuah sistem operasi yang spesifik). Internet adalah sumber informasi lain tentang kerentanan sistem yang diketahui yang diposkan oleh vendor, bersamaan dengan hot fixes, paket layanan tambalan, dan tindakan perbaikan lainnya yang dapat diterapkan untuk menghiliangkan atau mengurangi kerentanan. Sumber kerentanan terdokumentasi yang harus dipertimbangkan dalam analisis kerentanan, namun tidak terbatas pada, hal berikut:

a. Dokumentasi penilaian risiko sebelumnya dan sistemTI
b. Laporan audit sistem TI, laporan anomali sistem, laporan tinjauan keamanan, dan laporan pengujian dan evaluasi sistem
c. Kerentanan daftar, seperti NIST I-CAT kerentanan *database*
d. Saran keamanan, sepert FedCIRC dan buletin Kemampuan Penasihat Insentif

Komputer Departemen Energi

e. Saran vendor
f. Tim komando/tim tanggap darurat komputer komersial dan daftar pos (misal forum *SecurityFocus.com*)
g. Informasi *Assurance Vulnerablity Alerts* dan buletin untuk sistem militer
h. Analisis keamanan perangkat lunak sistem

2. Pengujian Keamanan Sistem

Metode proaktif, dengan menggunakan pengujian sistem, dapat digunakan untuk mengidentifikasi kerentanan sistem secara efisien, tergantung pada kekritisan sistem TI dan sumber daya yang ada (misal dana yang dialokasikan, teknologl yang tersedia. orang-orang yang memiliki keahlian untuk melakukan pengujan). Cara uji meliputi:

a. Alat pemindaian kerentanan otomatis
b. Uji dan evaluasi keamanan (ST & E)
c. Uji penetrasi

Alat pemindaian kerentanan olomatis digunakan untuk memindai sekelompok host atau jaringan untuk layanan rentan yang diketahui (misal sistem mengizinkan *Anonymous File Transfer Protocol* (FTP) *sendmail relaying*). Namun, perlu dicatat bahwa beberapa kerentanan potensial yang didentifikasi oleh alat pemindai otomatis mungkin tidak mewakili kerentanan nyata dalam konteks lingkungan sistem. Misalnya, beberapa alat pemindai ini memiliki potensi kerentanan potensial tanpa mempertimbangkan lingkungan dan persyaratan situs. Beberapa "kerentanan" yang ditandai oleh perangkat lunak pemindaian otomatis mungkin sebenamya tidak rentan terhadap situs tertentu namun dapat dikonfigurasi seperti itu karena lingkungan mereka memerlukanya. Dengan demikian, metode uji ini dapat menghasilkan fase positif.

ST & E adalah teknik lain yang dapat digunakan untuk mengidentifikasi kerentanan sistem TI selama proses penilaian risiko. Ini mencakup pengembangan dan pelaksanaan rencana pengujan (misal skrip uji, prosedur uji, dan hasl uji yang diharapkan). Tujuan pengujian keamanan sistem adalah menguji efektivitas

pengendalian

keamanan sistem Ti karena telah diterapkan di lingkungan operasional. Tujuannya adalah untuk memastikan bahwa kontrol yang diterapkan memenuhi spesifikasi keamanan yang disetujui untuk perangkat lunak dan perangkat keras dan menerapkan kebijakan keamanan organisasi atau memenuhi standar industri.

Pengujian penetrasi dapat digunakan unituk melangkapi tinjauan kontrol keamanan dan memastian bahwa berbagai aspek sistem TI diamankan. Pengujan penetrasi, bila digunakan dalam pioses penilalan risiko, dapat digunakan untuk menilai kemampuan sistem TI untuk menahan upaya yang disengeja untuk menghindari keamanan sistem. Tujuannya adalah untuk menguji sistem TI dari sudut pandang sumber ancaman dan untuk mengidentifikasi potensi kegagalan dalam skema perlindungan sistem TI. Hasil pengujian keamanan opsional jenis ini akan membantu mengidenitifikasi kerentanan sistem.

3. Pengembangan Daftar Periksa Persyaratan Keamanan

Selama tahap ini, personil penilaian risiko menentukan apakah persyaratan keamanan yang ditetapkan untuk sistem TI dan dikumpulkan selama karakterisasi sistem dipenuhi oleh kontrol keamanan yang ada atau yang direncanakan. Biasanya, persyaratan keamanan sistem dapat disajikan dalam bentuk tabel, dengan setlap persyaratan disertai penjelasan tentang bagaimana perancangan atau implementasi sistem dilakukan atau tidak menenuhi persyaratan pengendalian keamanan.

Daftar periksa persyaratan keamanan berisi standar keamanan dasar yang dapat digunakan untuk mengevaluasi dan mengidentifikasi kerentanan aset secara sistematis (personil, perangkat keras, perangkat lunak, informasi), prosedur, proses, dan transfer yang tidak terkait dengan sistem TI yang di area keamanan:

a. Manajemen
b. Operasional
c. Teknis

Tabel 2.4 mencantumkan kriteria keamanan yang disarankan untuk digunakan datam mengidentifikasi kerentanan sistem TI di setiap area keamanan.

Tabel 2.4
Kriteria Keamanan

Area Keamanan	Kriteria Keamanan
Keamanan manajemen	Penugasan tanggung jawab Kesinambungan dukungan Kemampuan respon insiden Peninjauan berkala atas kontrol keamanan Izin personil dan investigasi latar belakang Tugas berisiko Pelatihan keamanan dan teknis Pemisahan tugas Sistem otorisasi dan reauthorization Sistem atau rencana keamanan aplikasi
Keamanan Operasional	Pengendalian kontaminan yang mengandung udara (asap, debu, bahan kimia) Kontrol untuk memastikan kualitas daya listrik Akses dan pembuangan media data Distribusi data eksternal dan pelabelan Perlindungan fasilitas (misal ruang komputer, pusat data, kantor) Kontrol kelembaban Pengatur suhu Workstation, laptop, dan komputer pribadi
Keamanan teknis	Komunikasi Kriptografi Kontrol akses disrectionary Identifikasi dan otentikasi Deteksi gangguan Penggunaan kembali objek Audit sistem

Hasil dari proses ini adalah daftar periksa persyaratan keamanan. Sumber yang dapat digunakan untuk menyusun daftar periksa tersebut tidak terbatas pada perintah dan sumber peraturan permerintah yang berlaku untuk lingkungan pemrosesan sistem TI:

1. CSA tahun 1987
2. Publikasi Standar Pengolahan Informasi Federal
3. OMB November 2000 Edaran A-130
4. *Privacy Act* tahun 1974
5. Rencana keamanan sistem dari sistem TI

6. Kebijakan, pedoman, dan standar keamanan organisasi
7. Praktik industri

Panduan penilaian diri keamanan untuk sistem teknologi informasi memberikan kuesioner ekstensif yang bertujuan untuk pengendalian spesifik yang saling berhubungan. Tujuan pengendalian disarikan langsung dan persyaratan lama yang ditemukan dalam undang-undang, kebijakan, dan panduan mengenal keamanan dan privasi. Hasil *checklist* (atau kuesioner) dapat digunakan sebagai masukan untuk evaluasi kepatuhan dan ketidakpatuhan. Proses ini mengidentifikasi kelemahan sistem, proses dan prosedural yang mewakili potensi kerentanan.

Output dari Langkah 3 adalah daftar kerentanan sistem (observasi) yang dapat dilakukan oleh sumber ancaman potensial.

2.10.4 *Step 4 : Control Analysis* (Analisis Kontrol)

Tujuan dari langkah ini adalah untuk menganalisis kontrol yang telah dilaksanakan, atau direncanakan untuk diimplementasikan, oleh organisasi untuk meminimalkan atau menghilangkan kemungkinan ancaman yang menerapkan kerentanan sistem.

Untuk mendapatkan peringkat kemungkinan keseluruhan yang mengindikasikan probabilitas bahwa kerentanan polensial dapat diakukan dalam konstruksi lingkungan ancaman, pelaksanaan pengendalian saat ini atau yang direncanakan harus dipertimbangkan. Misal kerentanan (kelemahan sistem atau prosedural) kemungkinan rendah jika tingkat ancaman atau sumber ancaman rendah atau jika ada kontrol keamanan yang efektif yang dapat menghilangkan atau mengurangi besarnya bahaya.

1. Metode Kontrol

Kontrol keamanan mencakup penggunaan metode teknis dan nonteknis. Kontrol teknis adalah pengaman yang digabungkan ke perangkat keras, perangkat lunak, atau *firmware* komputer (misal mekanisme kontrol akses, mekanisme identifikasi dan otentikasi, metode enkripsi, perangkat lunak deteksi intrusi). Kontrol non teknis adalah

pengendalian manajemen dan operasional, seperi kebijakan keamanan, prosedur operasional, dan personil, fisik, dan keamanan lingkungan.

2. Kategori Kontrol

Kategori kontrol untuk metode kontrol teknis dan nonteknis dapat diklasifikasikan lebih jauh sebagai pencegahan atau detektf. Kedua subkategori ini dijelaskan sebagai berikut:

a. Kontrol pencegahan menghambat upaya untuk melanggar kebijakan keamanan dan mencakup kontrol seperti penegakan, enkripsi, dan otentikasi akses kontrol.
b. Kontrol detektif memperingatkan pelanggaran atau percobaan pelanggaran kebijakan keamanan dan mencakup kontrol sepert jalur audit, metode deteksi, intrusi, dan *checksum*.

Penerapan kontrol semacam itu salama proses mitigasi risiko adalah akibat langsung dari identfikasi kekurangan dalam pengendalian saat ini atau yang direncanakan selama proses penilaian risiko (misal kontrol tidak dilakukan atau tidak diterapkan dengan benar).

3. Teknik Analisis Kontrol

Pengembangan daftar persyaratan keamanan alau penggunaan daftar periksa yang tersedia akan sangat membantu dalam menganalisis pengendalian secara efisien dan sistematis. Daftar persyaratan keamanan dapat digunakan untuk memvalidasi katidakpatuhan keamanan dan kepatuhan. Oleh karena itu, penting untuk memperbarui daftar periksa terbebut untuk mencerminkan perubahan dalam lingkungan kontrol organisasi (misal perubahan dalam kebijakan keamanan, metode, dan persyaratan) untuk memastikan validitas daftar periksa.

Output dari Langkah 4 adalah daftar kontrol saat ini atau yang direncanakan yang digunakan untuk sistem TI untuk mengurangi kemungkinan adanya kerentanan yang dilakukan dan mengurangl dampak dari kejadian buruk tersebut.

2.10.5 *Step 5 : Likelihood Determination* (Kemungkinan Penentuan)

Untuk mendapatkan peringkat kemungkinan keseluruhan yang mengindikasikan probabilitas bahwa kerentanan potensial dapat dilakukan dalam konstruksi lingkungan ancaman terkait, faktor-faktor pengaturan berikut harus dipertimbangkan:

1. Motivasi dan kemampuan sumber ancaman
2. Sifat kerentanan
3. Keberadaan dan efektivitas kontrol saat ini

Kemungkinan bahwa potensi kerentanan dapat dilakukan oleh sumber ancaman tertentu dapat digambarkan dengan *High, Medium,* dan *Low.* Tabel 2.5 menggambarkan tiga tingkatan tersebut.

Tabel 2.5
Kemungkinan Definisi

Level	Kemungkinan Definisi
High	Sumber ancaman sangat termotivasi dan cukup mampu, dan kontrol untuk mencegah kerentanan tidak efektif.
Medium	Sumber ancaman dimotivasi dan mampu, namun kontrol bisa menghambat kerentanan.
Low	Sumber ancaman tidak memiliki motivasi atau kemampuan, atau bisa menghambat potensi kerentanan.

Output dari Langkah 5 adalah *likelihood rating (High, Medium, Low)*

2.10.6 *Step 6 : Impact Analysis* (Analisis Dampak)

Langkah utama berikutnya dalam mengukur tingkat risiko adalah menentukan dampak buruk akibat ancaman kerentanan terhadap ancaman yang berhasil. Sebelum memulai analisis dampak, perlu mendapatkan informasi penting berikut ini:

1. Misi sistem (misal proses yang dilakukan oleh sistem TI)
2. Kekritisan sistem dan data (misal nilai sistem atau kepentingan sebuah organisasi)
3. Sensitivitas sistem dan data.

Informasi ini dapat diperoleh dari dokumentasi organisasi yang ada, seperti laporan analisis dampak misi atau laporan penilaian kritikalitas aset. Analisis dampak misi

(juga dikenal sebagai analisis dampak bisnis [BIA] untuk beberapa organisasi) memprioriitaskan tingkat dampak yang terkait dengan kompromi aset informasi organisasi berdasarkan penilaian kualitatif atau kuantitatf terhadap sensitivitas dan kekritisan aset tersebut. Penilaian kritikalitas aset mengidentifikasi dan memprioritaskan aset informasi organisasi yang sensitif dan kritis (misal perangkat keras, perangkat lunak sistem, layanan, dan aset teknologi terkait) yarg mendukung misi kritis organisasi.

Jika dokumentasi ini tidak ada atau peniliaian untuk aset Ti organisasi tersebut belum dilakukan, kepekaan sistem dan data dapat ditentukan berdasarkan tingkat perindungan yang diperlukan untuk menjaga sistem dan ketersediaan data, integritas dan kerahasiaan. Teriepas dari metode yang digunakan untuk menentukan seberapa sensitf sistem TI dan datanya, pemilk sistem dan informasi bertanggung jawab untuk menentukan tingkat dampak sistem dan informasi mereka sendiri. Akibatnya dalam menganalisa dampaknya, pendekatan yang tepat adalah mewawancaral sistem dan pemilik informasi.

Oleh karena itu, dampak buruk dari kejadian keamanan dapat dijelaskan dalam hal kehilangan atau penurunan salah satu atau kombinasi dari salah satu dan tiga tujuan keamanan berikut: integritas, ketersediaan, dan kerahasiaan. Daftar berikut ini memberikan deskripsi singkat tentang setiap tujuan keamanan dan konsekuensi (atau dampaknya) yang tidak terpenuhi:

1. Kehilangan Integritas. Integritas sistem dan data mengacu pada persyaratan bahwa informasi dilindungi dari modifikasi yang tidak benar. Integritas hilang jika perubahan yang tidak sah dilakukan terhadap data atau sistem TI dengan tindakan yang disengaja atau tdak disengeja Jika kehilangan integriitas sistem

atau data tidak dikoreksi, penggunaan sistem yang terkontaminasi atau data yang rusak dapat mengakibatkan ketidakakuratan, kecurangan, atau keputusan yang keliru. Juga pelanggaran integritas mungkin merupakan langkah awal dalam serangan yang berhasil melawan ketersediaan atau kerahasiaan sistem. Untuk semua alasan ini, kehilangan integritas mengurangi kepastian sistem TI.

2. Kehilangan Ketersediaan. Jika sisten TI *mission-critical* tidak tersedia bagi pengguna akhir, misi organisasi mungkin akan terpengaruh. Hilangnya fungsionalitas sistem dan efektivilas operasional, misalnya, dapat mengakibatkan hilangnya waktu produkif, sehingga menghambat kinerja pengguna akhir fungsi mereka dalam mendukung misi organisasi.
3. Hilangnya Kerahasiaan. Sistem dan kerahasiaan data mengacu pada perlindungan informasi dari pengungkapan yang tidak sah. Dampak pengungkapan informasi rahasia yang tidak sah dapat berkisar dari membahayakan keamanan nasional hingga pengungkapan data *Privacy Act*. Pengungkapan yang tidak sah, tidak diantisipasi, atau tidak disengaja dapat mengakibatkan hilangnya kepercayaan publik, rasa malu, atau indakan hukum terhadap organisasi.

Beberapa dampak nyata dapat diukur secara kuantitatif seperti kehilangan pendapatan, biaya perbaikan sistem, atau tingkat usaha yang diperlukan untuk memperbaiki masalah yang disebabkan oleh tindakan ancaman. Dampak lainnya (misal hilangnya kepercayaan masyarakat, kehilangan kredibilitas, kerusakan pada kepentingan organisasi) tidak dapat diukur namun dapat dikualifikasi atau dijelaskan dalam *High*, *Medium*, dan *Low*. Panduan ini hanya menjelaskan kategori kualitatif dampak *High*, *Medium*, dan *Low* seperti yang terdapat pada Tabel 2.6.

Tabel 2.6
Besaran Definisi Dampak

Level	Kemungkinan Definisi
High	(1) dapat menyebabkan hilangnya aset atau sumber daya; (2) dapat secara signifikan melanggar, atau menghalangi misi, atau kepentingan organisasi; atau (3) dapat mengakibatkan kematian manusia atau cedera serius.

Medium	(1) dapat mengakibatkan hilangnya sumber daya atau sumber daya; (2) dapat merugikan, atau menghalangi misi, reputasi, atau kepentingan organisasi; atau (3) dapat mengakibatkan cedera manusia.
Low	(1) dapat mengakibatkan hilangnya beberapa aset atau sumber daya atau (2) dapat mempengaruhi misi, reputasi, atau kepentingan organisasi.

1. Penilaiain Kuantitatif Versus Penilaian Kualitatif

Dalam melakukan analisis dampak, pertimbangan harus diberikan pada keuntungan dan kerugian dari penilaian kuantitatif versus kualitatif. Keuntungan utama analisis dampak kualitatif adalah bahwa ia memprioritaskan risiko dan mengidentifikasi area untuk segera diperbaiki dalam mengatasi kerentanan. Kerugian dari analis kualitatif adalah bahwa ia tidak memberikan pengukuran kuantitatif yang dapat diukur dari besaran dampaknya, sehingga membuat analisis biaya manfaat dari setiap kontrol yang direkomendasikan sulit dilakukan.

Keuntungan utama analisis dampak kuantitatif adalah pengukuran tingkat dampak yang dapat digunakan dalam analisis biaya manfaat dari kontrol yang direkomendasikan. Kelemahannya adalah, tergantung pada rentang numerik yang digunakan untuk mengekspresikan pengukuran, makna analisis dampak kuantitatif mungkin tidak jelas, yang memerlukan hasil untuk ditafsirkan secara kualitatif. Faktor tambahan sering harus dipertimbangkan untuk menentukan besamya dampak. Ini mungkin termasuk namun tdak terbatas pada:

a. Estimasi frekuensi kerentanan sumber ancaman terhadap kerentanan tersebut selama jangka waktu tertentu (misalnya 1 tahun)
b. Perkiraan biaya untuk setiap kejadian latihan sumber ancaman kerentanan
c. Faktor tertimbang berdasarkan analisis subjektif dampak relatif ancaman spesifik yang menggunakan kerentanan spesifik

Output dari Langkah 6 adalah besaran dampak *(High*, *Medium*, dan *Low).*

2.10.7 *Step 7 : Risk Determination* (Penentuan Risiko)

Tujuan dari langkah ini adalah untuk menilai tingkat risiko terhadap sistem TI. Penentuan risiko pasangan ancaman/kerentanan tertentu dapat dinyatakan sebagai fungsi dari:

1. Kemungkinan sumber ancaman tertentu mencoba menerapkan kerentanan tertentu
2. Besarnya dampaknya jika sumber ancaman berhasil menjalankan kerentanan tersebut
3. Kecukupan kontrol keamanan yang direncanakan atau yang sudah ada untuk mengurangi atau menghilangkan risiko.

Untuk mengukur risiko, skala risiko dan matriks tingkat risiko harus dikembangkan.

1. Matriks Tingkat Risiko

Penentuan akhir risikto misi diturunkan dengan mengalikan peringkat yang ditetapkan untuk kemungkinan ancaman (misal probabilitas) dan dampak ancaman. Tabel 2.7 dibawah ini menunjukan bagaimana keseluruhan penilaian risiko dapat ditentukan berdasarkan masukan dari kategon kemungkinan ancaman dan kategori ancaman. Matrks dibawah ini adalah matriks kemungkinan ancaman 3x3 *(High, Medium,* dan *Low)* dan dampak ancaman *(High, Medium,* dan *Low)*. Bergantung pada persyaratan situs dan granularitas penilaian risiko yang diïinginkan, beberapa situs mungkin menggunakan matriks 4 x 4 atau 5 x 5. Yang terakhir ini dapat mencakup kemungkinan ancaman sangat rendah/sangat tinggi dan dampak sangat rendah/sangat tinggi untuk menghasilkan tingkat risiko sangat rendah/sangat tinggi. Tingkat risiko "sangat tinggi" mungkin memerlukan kemungkinan penghentian sistem atau penghentian semua integrasi dan upaya pengujian sistem TI.

Matriks sampel pada Tabel 2.7 menunjukkan bagaimana tingkat risiko keseluruhan *High, Medium,* dan *Low* diturunkan. Penentuan tingkat risiko atau penilaian ini mungkin subjektif. Dasar pemikiran untuk pembenaran ini dapat dijelaskan dalam hal probabilitas yang ditetapkan untuk setiap tingkat kemungkinan ancaman dan nilal yang ditetapkan untuk setiap tingkat dampak. Sebagai contoh:

a. Probabilitas yang ditetapkan untuk setiap tingkat kemungkinan ancaman adalah 1,0 untuk *High*, 0,5 untuk *Medium*, 0,1 untuk *Low.*

b. Nilai yang ditetapkan untuk setiap tingkat dampak adalah 100 untuk Tinggi, 50 untuk *Medium*, dan 10 untuk *Low*.

Tabel 2.7
Matriks Tingkat Risiko

Threat / ***Likelihood***	***Impact*** ***Low*** **(10)**	***Medium*** **(50)**	***High*** **(100)**
High **(1.0)**	*Low* 10 X 1.0 = 10	*Medium* 50 X 1.0 = 50	*High* 100 X 1.0 = 100
Medium **(0.5)**	*Low* 10 X 0.5 = 5	*Medium* 50 X 0.5 = 25	*Medium* 100 X 0.5 = 50
Low **(0.1)**	*Low* 10 X 0.1 = 1	*Low* 50 X 0.1 = 5	*Low* 100 X 0.1 = 10

2. Deskripsi Tingkat Risiko

Tabel 2.8 menjelaskan tingkat risiko yang ditunjukkan pada matriks sebelumnya.

Tabel 2.8
Skala Risiko dan Tindakan yang Diperlukan

Level	Deskripsi Risiko dan Tindakan yang Diperlukan
High	Jika pengamatan atau temuan dievaluasi sebagai risiko tinggi, ada kebutuhan yang kuat untuk tindakan perbaikan. Sistem yang ada mungkin terus beroperasi, namun rencana tindakan korektif harus dilakukan sesegera mungkin.
Medium	Jika pengamatan dinilai sebagai risiko menengah, tindakan perbaikan diperlukan dan sebuah rencana harus dikembangkan untuk memasukkan tindakan ini dalam jangka waktu yang wajar.
Low	Jika pengamatan digambarkan sebagai risiko rendah, sistem harus menentukan apakah tindakan perbaikan masih diperlukan atau memutuskan untuk menerima risikonya.

Output dari Langkah 7 adalah tingkat risiko *(High, Medium, Low)*.

2.10.8 *Step 8 : Control Recommendations* (Rekomendasi Kontrol)

Selama tahap proses ini, kontrol yang dapat mengurangi atau menghilangkan risiko yang teridentifikasi, yang sesuai dengan operasi organisasi disediakan. Tujuan dari kontrol yang direkomendasikan adalah mengurangi tingkat risiko terhadap sistem TI dan datanya ke tingkat yang dapat diterima. Faktor-faktor berikut harus dipertimbangkan dalam merekomendasikan kontrol dan solusi alternatif untuk meminimalkan atau menghilangkan risiko yang teridentifikasi:

1. Efektivitas pilihan yang disarankan (seperti kompatibilitas sistem)
2. Perundang-undangan dan peraturan
3. Kebijakan organisasi
4. Dampak operasional
5. Keselamatan dan keandalan

Rekomendasi pengendalian adalah hasil dari proses penilaian risiko dan memberikan masukan terhadap proses mitigasi risiko, dimana kontrol keamanan prosedural dan teknis yang direkomendasikan dievaluasi, diprionitaskan, dan diterapkan. Perlu dicatat bahwa tidak semua kemungkinan kontrol yang direkomendasikan dapat dimplementasikan untuk mengurangi kerugian untuk menentukan mana yang dibutuhkan dan sesuai untuk organisasi tertentu, analisis biaya manfaat harus dilakukan untuk pengendalian rekomendasi yang disarankan, untuk menunjukkan bahwa biaya penerapan kontrol dapat dibenarkan oleh pengurangan tingkat risiko. Selain itu, dampak operasional (misal berpengaruh pada kinerja sistem) dan kelayakan (misal persyaratan teknis, penerimaan pengguna) untuk memperkenalkan opsi yang disarankan harus dievaluasi secara hati-hati selama proses mitigasi risiko.

Output dari Langkah 8 adalah rekomendasi pengendalian dan solusi

alternatif untuk mengurangi risiko

2.10.9 *Step 9 : Results Documentation* (Hasil Dokumentasi)

Setelah penilaian risiko selesai (ancaman dan kerentanan diidentifikasi, risiko dinilai, dan kontrol yang direkomendasikan yang diberikan), hasilnya harus didokumentasikan dalam laporan resmi atau pengarahan.

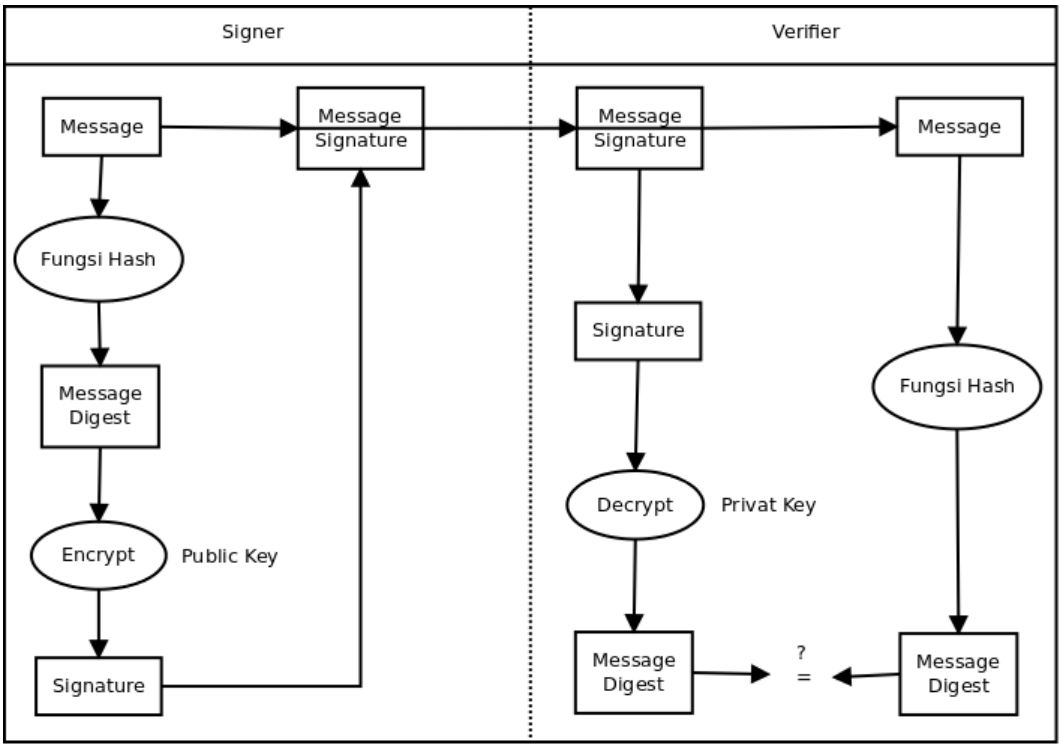
Laporan penilaian risiko adalah laporan manajenen yang membantu manajemen senior yaitu pemilik misi, membuat keputusan mengenai perubahan kebijakan, prosedural, anggaran, dan sistem dan manajemen. Tidak seperti laporan audit atau investigasi, yang mencari kesalahan, laporan penilaian risiko seharusnya tdak diajukan dengan cara yang menuduh, tetapi sebagai pendekatan sistematis dan analitis untuk menilai risiko sehingga manajemen senior akan memahami risiko dan mengalokasikan sumber daya untuk mengurangi dan memperbaiki potensi kerugian. Untuk alasan ini, beberapa orang lebih memilih untuk menangani pasangan ancaman/kerentanan karena pengamatan, bukan temuan dalam laporan penilaian nisiko.

Output dari Langkah 9 adalah laporan penilaian risiko yang menggambarkan ancaman dan kerentanan, mengukur risiko, dan memberikan rekomendasi untuk pelaksanaan pengendalian.

BAB III
OBJEK DAN METODOLOGI PENELITIAN

3.1 *Digital Signature*

Objek penelitian yang digunakan dalam penelitian ini adalah *digital signature.* Dalam *digital signature* ada yang disebut dengan *signer* dan *verifier. Signer* merupakan pengirim pesan (pemberi tanda tangan *digital* pada pesan) sedangkan *verifier* adalah penerima pesan (pemverifikasi pesan). Skema *digital signature* merupakan tahap pertama pada proses *risk assessment* yaitu tahap *system characterization*. Skema otentikasi *digital signature* oleh *signer* dan *verifier* yang bisa dilihat pada Gambar 3.1.



Gambar 3.1
Skema Otentikasi Digital Signature (Munir, 2004)

Dibawah ini merupakan tabel deskripsi dari skema otentikasi *digital signature* yang dapat dilihat pada pada Tabel 3.1.

Tabel 3.1
Deskripsi Skema Otentikasi Digital Signature

No.	*Subject*	*Descryption*
1.	*Signer*	1. Pesan yang akan dikirimkan kepada penerima dilakukan proses hash terlebih dahulu. 2. Pesan yang telah dihash akan berubah menjadi *message digest.* *3. Message Digest* tersebut dienkripsi menggunakan kunci publik (dalam penelitian ini pesan dienkripsi mengunakan Hill *Cipher*). 4. Hasil dari proses enkripsi akan menghasilkan *digital signature.* 5. Pesan asli dan *digital signature* dikirim bersamaan kepada si penerima pesan,
2.	*Verifier*	1. Pesan asli dan *digital signature* yang diterima secara bersamaan dipisah oleh sipenerima pesan. 2. *Digital signature* yang diterima dilakukan proses dekripsi menggunakan kunci rahasia/*private* (dalam penelitian ini pesan didekripsi mengunakan Hill *Cipher*). *3. Digital signature* yang sudah didekripsi akan menghasilkan *message digest.* 4. Pesan asli yang diterima dilakukan proses *hash* 5. Pesan asli yang sudah di *hash* akan menghasilkan *message digest* 6. Cek apakah *message digest* yang dihasilkan oleh *digital signature* sama dengan *message digest* yang dihasilkan oleb pesan asli.

3.2 Kriptografi Hill *Cipher*

Pada skema *digital signature* di atas, terdapat proses enkripsi dan dekripsi yang dilakukan setelah melakukan proses *hash*. Dalam penelitian ini teknik yang akan digunakan untuk enkripsi dan dekripsi adalah teknik algoritma Hill *Cipher*. Hill *Cipher* diciptakan oleh Lester S. Hill pada tahun 1929. Hill *Cipher* menggunakan operasi aljabar linier matriks n x n untuk mengenkripsi dan mendekripsi pesannya. Berikut ini adalah contoh penerapan enkripsi dan dekripsi Hill *Cipher* dengan kunci matriks berordo 2x2.

3.2.1 Enkripsi Hill *Cipher*

Enkripsi merupakan proses merubah pesan asli (*plaintext*) menjadi pesan sandi (*ciphertext*). Proses enkripsi dilakukan untuk menyamarkan pesan agar tidak diketahui oleh pihak lain selain si penerima pesan. Langkah-langkah enkripsinya adalah sebagai berikut:

1. Tabel Definisi Hill *Cipher*

Hal yang perlu dipersiapkan sebelum melakukan enkripsi yaitu menyediakan tabel definisi Hill *Cipher*. Tabel definisi Hill *Cipher* dapat dilihat pada tabel 3.2.

Tabel 3.2
Definisi Hill Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

2. Kunci Hill *Cipher*

Langkah selanjutnya adalah menentukan kunci Hill *Cipher* yang akan digunakan pada saat enkripsi. Syarat penggunaan kunci matriks pada Hill *Cipher* adalah determinan nya harus bernilai satu.

$$K = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$$

3. Plaintext

Hal berikutnya yang dilakukan adalah menentukan *plaintext* yang akan dienkripsi. *Plaintext* tersebut harus dibagi menjadi masing-masing dua blok karakter. Setelah dibagi menjadi dua blok karakter, selanjutnya adalah subtitusi *plaintext* tersebut ke dalam angka. Setelah itu periksa jumlah karakter atau huruf *plaintext* yang akan di enkripsi. Apabila huruf *plaintext*-nya berjumlah ganjil tambahkan satu huruf dibelakang kata. Dalam penelitian ini *plaintext* yang digunakan adalah kata “LIKMI” yang berjumlah lima huruf. Karena *plaintext*-nya berjumlah ganjil, maka harus ditambahkan satu huruf dibelakang kata “LIKMI”. Dalam penelitian ini huruf yang akan ditambahkan di belakang kata adalah huruf “Z”. Dalam tabel definisi, huruf “Z” mendapatkan nilai tertinggi, sehingga dalam proses enkripsi diharapkan huruf “Z” tersebut akan bergeser jauh dari huruf aslinya.

$$\begin{bmatrix} L \\ I \end{bmatrix} = \begin{bmatrix} 11 \\ 8 \end{bmatrix} \qquad \begin{bmatrix} I \\ Z \end{bmatrix} = \begin{bmatrix} 8 \\ 25 \end{bmatrix}$$

$$\begin{bmatrix} K \\ M \end{bmatrix} = \begin{bmatrix} 10 \\ 12 \end{bmatrix}$$

4. Implementasikan ke dalam rumus Hill *Cipher*

Langkah selanjutnya adalah mengimplementasikan kunci dan *plaintext* kedalam rumus Hill *Cipher* yaitu C = K.P mod 26. Dengan definisinya C adalah *ciphertext* yang ingin dicari, K adalah kunci Hill *Cipher* yang digunakan, dan P adalah *plaintext.*

$$\begin{bmatrix} L \\ I \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 11 \\ 8 \end{bmatrix} = \begin{bmatrix} 46 \\ 27 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 20 \\ 1 \end{bmatrix} = \begin{bmatrix} U \\ B \end{bmatrix}$$

$$\begin{bmatrix} K \\ M \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 10 \\ 12 \end{bmatrix} = \begin{bmatrix} 56 \\ 34 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 4 \\ 8 \end{bmatrix} = \begin{bmatrix} E \\ I \end{bmatrix}$$

$$\begin{bmatrix} I \\ Z \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 8 \\ 25 \end{bmatrix} = \begin{bmatrix} 91 \\ 58 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 13 \\ 6 \end{bmatrix} = \begin{bmatrix} N \\ G \end{bmatrix}$$

5. Hasil enkripsi

Kata yang dihasilkan setelah melakukan proses enkripsi di atas adalah kata “UBEING”. Proses enkripsi tersebut dikatakan berhasil karena kata “LIKMIZ” sudah berubah menjadi “UBEING”.

3.2.2 Dekripsi Hill *Cipher*

Dekripsi merupakan proses merubah pesan sandi (*ciphertext*) kembali menjadi pesan asli (*plaintext*). Proses dekripsi dilakukan untuk mengembalikan pesan hasil enkripsi sebelumnya agar kembali menjadi pesan asli yang mempunyai makna. Langkah-langkah dekripsinya adalah sebagai berikut:

1. Tabel Definisi Hill *Cipher*

Hal yang perlu dipersiapkan sebelum melakukan dekripsi yaitu menyediakan tabel definisi Hill *Cipher* yang sama dengan pada saat proses enkripsi. Tabel definisi Hill *Cipher* dapat dilihat pada tabel 3.3.

Tabel 3.3
Definisi Hill Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

2. Kunci Hill *Cipher*

Langkah selanjutnya adalah menentukan kunci Hill *Cipher* yang akan digunakan untuk proses dekripsi. Kunci yang digunakan adalah kunci hasil *inverse* pada saat enkripsi.

$$K^{-1} = \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix}$$

3. Ciphertext

Hal berikutnya yang dilakukan adalah menentukan *ciphertext* yang akan didekripsi. Dalam penelitian ini *ciphertext* yang digunakan adalah kata "UBEING" hasil proses enkripsi sebelumnya. Bagi *ciphertext* tersebut menjadi masing-masing dua blok karakter. Setelah dibagi menjadi dua blok karakter, selanjutnya adalah subtitusi *ciphertext* tersebut ke dalam angka.

$$\begin{bmatrix} U \\ B \end{bmatrix} = \begin{bmatrix} 20 \\ 1 \end{bmatrix} \qquad \begin{bmatrix} N \\ G \end{bmatrix} = \begin{bmatrix} 13 \\ 6 \end{bmatrix}$$

$$\begin{bmatrix} E \\ I \end{bmatrix} = \begin{bmatrix} 4 \\ 8 \end{bmatrix}$$

4. Implementasikan ke dalam rumus Hill *Cipher*

Langkah selanjutnya adalah mengimplementasikan kunci dan *ciphertext* kedalam rumus Hill *Cipher* yaitu $P = K^{-1}.C \bmod 26$. Dengan definisinya P adalah *plaintext* yang ingin dicari, K^{-1} adalah kunci Hill *Cipher* yang digunakan, dan C adalah *ciphertext.*

$$\begin{bmatrix} U \\ B \end{bmatrix} = \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix} . \begin{bmatrix} 20 \\ 1 \end{bmatrix} = \begin{bmatrix} 37 \\ -18 \end{bmatrix} \bmod 26 = \begin{bmatrix} 11 \\ 8 \end{bmatrix} = \begin{bmatrix} L \\ I \end{bmatrix}$$

$$\begin{bmatrix} E \\ I \end{bmatrix} = \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix} . \begin{bmatrix} 4 \\ 8 \end{bmatrix} = \begin{bmatrix} -16 \\ 12 \end{bmatrix} \bmod 26 = \begin{bmatrix} 10 \\ 12 \end{bmatrix} = \begin{bmatrix} K \\ M \end{bmatrix}$$

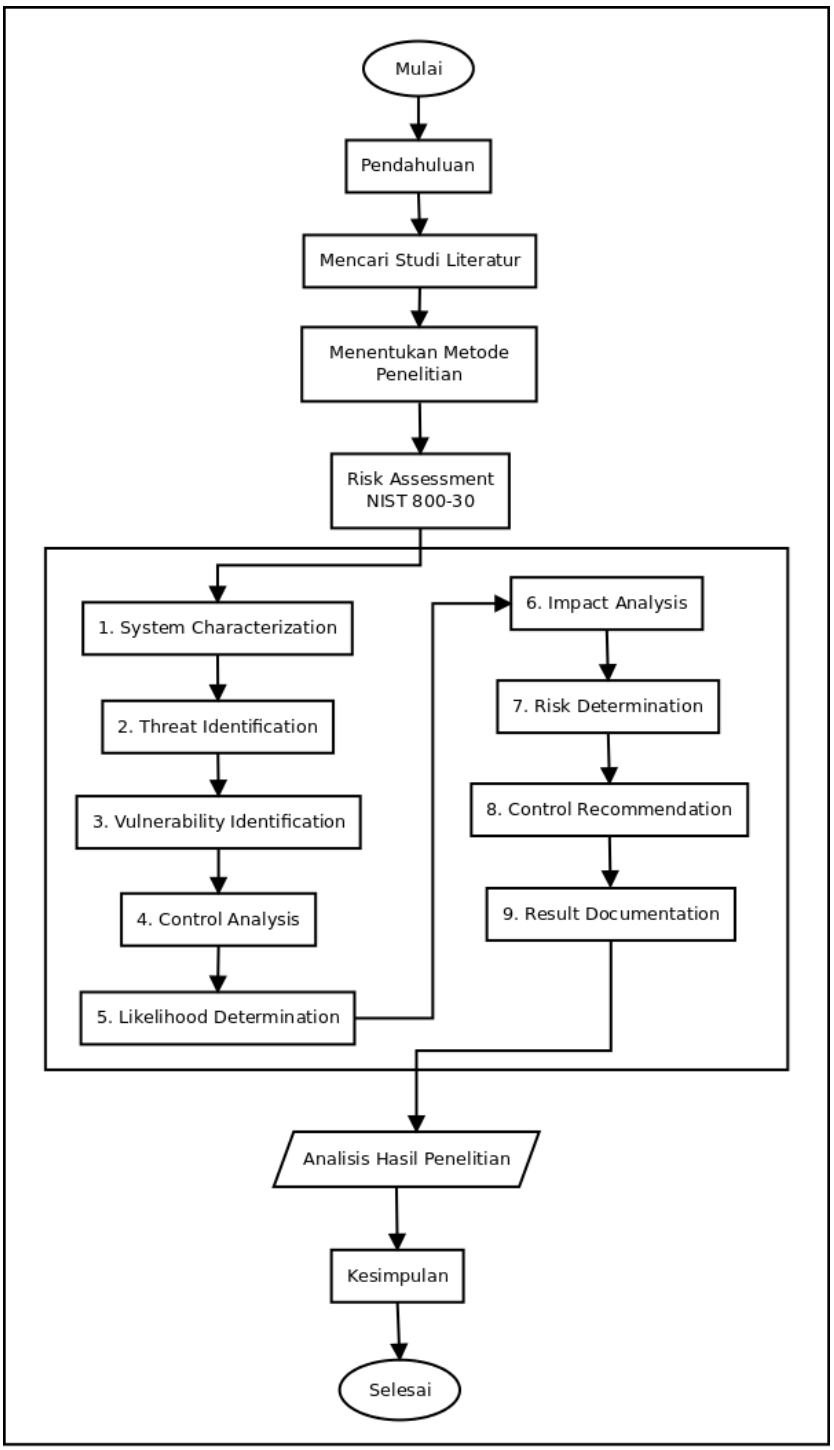
$$\begin{bmatrix} N \\ G \end{bmatrix} = \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix} . \begin{bmatrix} 13 \\ 6 \end{bmatrix} = \begin{bmatrix} 8 \\ -1 \end{bmatrix} \bmod 26 = \begin{bmatrix} 8 \\ 25 \end{bmatrix} = \begin{bmatrix} I \\ Z \end{bmatrix}$$

5. Hasil dekripsi

Kata yang dihasilkan setelah melakukan proses dekripsi di atas adalah kata "LIKMIZ". Proses dekripsi tersebut dikatakan berhasil karena kata "UBEING" sudah kembali menjadi pesan aslinya yaitu kata "LIKMI".

3.3 Alur Metodologi Penelitian

Berikut adalah langkah-langkah yang dilakukan dalam melakukan penelitian yang dapat dilihat pada Gambar 3.2.



Gambar 3.2
Alur Metodologi Penelitian

Berikut merupakan tabel deskripsi dari alur metodologi penelitian yang dapat dilihat pada pada Tabel 3.4.

Tabel 3.4
Deskripsi Alur Metodologi Penelitian

No.	*Step*	*Descryption*
1.	Pendahuluan	Mencari latar belakang penggunaan *digital signature* kriptografi Hill *Cipher,* identifikasi masalah mengenai kerentanan *digital signature* kriptografi Hill *Cipher,* dan menentukan batasan-batasan penelitian.
2.	Mencari Studi Literatur	Mencari studi literatur mengenai *Entity Authentication, Information Security Objective,* Tanda Tangan, *Digital Signature,* Kriptografi, Kriptografi Hill *Cipher*, *Security Attack Model, Cryptanalysis,* dan *Risk Assessment*
3.	Menentukan Metodologi Penelitian	Melakukan analisis terhadap metodologi penelitian yang digunakan yaitu teknik *risk assessment* berdasarkan NIST 800-30.
4.	*Risk Assessment* dengan NIST 800-30	Melakukan *risk assessment* terhadap kerentanan *digital signature* kriptografi Hill *Cipher* dengan melakukan langkah-langkah yang terdapat pada NIST 800-30.
a.	*System Characterization*	Mencari tahu karakteristik sistem cara kerja otentikasi pesan menggunakan *digital signature* kriptografi Hill *Cipher.*
b.	*Threat Identification*	Melakukan identifikasi ancaman yang dapat menyerang *digital signature* kriptografi Hill *Cipher.*
c.	*Vulnerability Identification*	Melakukan identifikasi kerentanan atau kelemahan-kelemahan yang ada pada *digital signature* kriptografi Hill *Cipher.*
d.	*Control Analysis*	Melakukan analisis kontrol atau pencegahan yang akan dilakukan.
e.	*Likelihood Determination*	Melakukan identifikasi sumber ancaman yang menyerang kerentanan atau kelemahan-kelemahan pada *digital signature* kriptografi Hill *Cipher.*
f.	*Impact Analysis*	Melakukan analisis dampak-dampak yang akan terjadi akibat kerentanan yang terdapat pada *digital signature* kriptografi Hill *Cipher.*
g.	*Risk Determination*	Penentuan risiko-risiko yang akan muncul kemudian hari akibat kerentanan yang ada pada *digital signature* kriptografi Hill *Cipher*
h.	*Control Recommendations*	Menentukan rekomendasi kontrol yang akan dilakukan untuk mencegah risiko-risiko yang terjadi pada *digital signature* kriptografi Hill *Cipher.*
i.	*Results Documentation*	Melakukan dokumentasi dari hasil penelitian.
5.	Analisis Hasil Penelitian	Mengkaji ulang hasil peneilitian.
6.	Kesimpulan	Membuat kesimpulan hasil peneilitian.

3.4 *Risk Assessment* (Penilaian Risiko) dengan NIST 800-30

Dalam penelitian ini objek yang akan dianalisis adalah penilaian risiko terhadap *digital signature* kriptografi Hill *Cipher* dan kerentanannya. Keluaran dari proses ini membantu mengidentifikasi pengendalian yang tepat untuk mengurangi atau menghilangkan risiko penggunaan *digital signature* kriptografi Hill *Cipher* terhadap kerentannya. Tahapan *risk assessment* yang dilakukan berdasarkan NIST 800-30 (Stoneburner., dkk. 2002) adalah:

1. *Step 1 : System Characterization* (Karakterisasi Sistem)
2. *Step 2 : Threat Identification* (Identifikasi Ancaman)
3. *Step 3 : Vulnerability Identification* (Identifikasi Kerentanan)
4. *Step 4 : Control Analysis* (Analisis Kontrol)
5. *Step 5 : Likelihood Determination* (Kemungkinan Penentuan)
6. *Step 6 : Impact Analysis* (Analisis Dampak)
7. *Step 7 : Risk Determination* (Penentuan Risiko)
8. *Step 8 : Control Recommendations* (Rekomendasi Kontrol)
9. *Step 9 : Results Documentation* (Hasil Dokumentasi)

3.4.1 *Step 1 : System Characterization* (Karakterisasi Sistem)

Langkah pertama yang dilakukan adalah menentukan ruang lingkup sistem yang akan dianalisis. Sistem yang akan dianalisis dalam penelitian ini adalah teknik otentikasi pesan menggunakan *digital signature* kriptografi Hill *Cipher*. Pada tahap ini sistem atau cara kerja teknik otentikasi pesan menggunakan *digital signature* kriptografi Hill *Cipher* diidentifikasi.

3.4.2 *Step 2 : Threat Identification (*Identifikasi Ancaman*)*

Kendala yang dihadapi oleh pesan yang sudah ditandatangani oleh *digital signature* kriptografi Hill *Cipher* saat ini yang sudah diketahui adalah serangan kriptanalisis. Kriptanalisis merupakan ilmu dan (terkadang disebut seni) untuk

memecahkan kriptosistem. Kriptanalisis sangat penting bagi kriptosistem modern, karena tanpa kriptanalisis kriptosistem yang digunakan tidak akan diketahui apakah sudah aman atau masih ada celah pada sistem keamanannya. Pada langkah ini, kerentanan pada Hill *Cipher* yang mengancam keaslian pesan akan dianalisis.

3.4.3 *Step 3 : Vulnerability Identification* (Identifikasi Kerentanan)

Berdasarkan identifikasi ancaman yang telah dilakukan, langkah selanjutnya yang akan dilakukan adalah mengidentifikasi kerentanan terhadap pesan yang sudah ditandatangani oleh *digital signature* kriptografi Hill *Cipher.* Kerentanan yang akan dianalisa dalam penelitian ini adalah kerentanan pesan ketika sudah ditandatangani oleh *digital signature* kriptografi Hill *Cipher* berdasarkan ketersediaan data dan berdasarkan kunci Hill *Cipher* yang akan dipakai dalam proses enkripsi dan dekripsinya.

3.4.4 *Step 4 : Control Analysis* (Analisis Kontrol)

Selanjutnya adalah mengidentifikasi kontrol yang harus dilakukan pada pesan yang sudah ditandatangani oleh *digital signature* kriptografi Hill *Cipher*. Kontrol yang perlu dilakukan adalah dengan mencegah agar potongan pesan tersebut sebisa mungkin tidak ditemukan oleh oranglain yang tidak berhak mengakses pesan tersebut. Selain potongan pesan, kunci yang digunakan untuk enkripsi dan dekripsi pesan perlu dirahasiakan untuk mencegah kebocoran pesan.

3.4.5 *Step 5 : Likelihood Determination* (Kemungkinan Penentuan)

Langkah selanjutnya yaitu menentukan kemungkinan potensi kerentanan terhadap pesan yang sudah ditandatangai oleh *digital signature* kriptografi Hill *Cipher*. Kemungkinan potensi kerentanan pesan tersebut terhadap kriptanalisis dapat digambarkan dengan tingkat *high, medium,* dan *low*.

3.4.6 *Step 6 : Impact Analysis* (Analisis Dampak)

Dampak yang diakibatkan oleh kerentanan Hill *Cipher* dapat menimbulkan kerugian seperti rusaknya integritas dan hilangnya kerahasiaan pesan yang sudah ditandatangani menggunakan *digital signature* kriptografi Hill *Cipher*. Kerusakan pada pesan akibat kerentanan tersebut tidak dapat diukur secara kuantitatif namun dapat dikualifikasi dalam *high, medium,* dan *low* dalam penggambarannya*.*

3.4.7 *Step 7 : Risk Determination* (Penentuan Risiko)

Selanjutnya adalah menentukan risiko dari kerentanan Hill *Cipher* terhadap pesan yang sudah ditandatangani menggunakan *digital signature* kriptografi Hill *Cipher*. Penentuan risiko terhadap pesan tersebut terhadap kerentanannya dapat dilakukan dengan menggunakan matriks tingkat risiko dan deskripsi tingkat risiko. Matriks yang digunakan adalah matriks dengan ordo 3 x 3, dan variabel tingkatan yang digunakan adalah *high, medium,* dan *low.*

Matriks pada Tabel 3.5 menunjukkan tingkat risiko keseluruhan. Penentuan tingkat risiko atau penilaian ini bersifat subjektif. Pemberian bobotnya digambarkan sebagai berikut:

1. Probabilitas yang ditetapkan untuk setiap tingkat kemungkinan ancaman adalah 1,0 untuk *High*, 0,5 untuk *Medium*, 0,1 untuk *Low.*
2. Nilai yang ditetapkan untuk setiap tingkat dampak adalah 100 untuk *High*, 50 untuk *Medium*, dan 10 untuk *Low*.

Tabel 3.5
Matriks Tingkat Risiko

Threat	**Impact**		
Likelihood	**Low (10)**	**Medium (50)**	**High (100)**
High (1.0)	Low 10 X 1.0 = 10	Medium 50 X 1.0 = 50	High 100 X 1.0 = 100
Medium (0.5)	Low 10 X 0.5 = 5	Medium 50 X 0.5 = 25	Medium 100 X 0.5 = 50
Low (0.1)	Low 10 X 0.1 = 1	Low 50 X 0.1 = 5	Low 100 X 0.1 = 10

3.4.8 *Step 8 : Control Recommendations (Rekomendasi Kontrol)*

Langkah ini berisi daftar kontrol yang akan direkomendasikan. Kontrol yang akan direkomendasikan bertujuan untuk mengurangi tingkat risiko terhadap pesan yang sudah ditandatangani menggunakan *digital signature* kriptografi Hill *Cipher* ke tingkat yang dapat diterima. Sebelum diimplementasikan, kontrol yang direkomendasikan perlu dianalisis sesuai dengan kebutuhan. Analisis yang dilakukan seperti analisis kebutuhan terhadap integritas dan kerahasiaan pesan pada saat proses pengiriman pesan ketika sudah ditandatangani oleh *digital signature* kriptografi Hill *Cipher*.

3.4.9 *Step 9 : Results Documentation* (Hasil Dokumentasi)

Setelah penilaian risiko selesai hasilnya didokumentasikan dalam bentuk laporan. Laporan penilaian risiko dibuat sebagai pendekatan sistematis dan analitis untuk menilai risiko terhadap pesan yang sudah ditandatangani menggunakan *digital signature* kriptografi Hill *Cipher.* Hal tersebut perlu dilakukan sehingga risiko dan teknik yang akan dilakukan untuk mengurangi dan memperbaiki potensi kerugian dari pesan yang sudah ditandatangani menggunakan *digital signature* kriptografi Hill *Cipher* tersebut dapat dipahami dan diimplementasikan.

BAB IV
HASIL DAN PEMBAHASAN

4.1 *Step 1 : System Characterization* (Karakterisasi Sistem)

Sistem yang akan di analisa dalam penelitian adalah *digital signature* kriptografi Hill *Cipher*. Sistem atau cara kerja *digital signature* kriptografi Hill *Cipher* sudah digambarkan pada saat menjelaskan objek penelitian pada bab sebelumnya.

4.2 *Step 2 : Threat Identification (*Identifikasi Ancaman*)*

Serangan yang mengancam *digital signature* kriptografi Hill *Cipher* yang diketahui adalah kriptanalisis Hill *Cipher* dengan *mathematic analysis* yaitu teknik kriptanalisis dengan menggunakan analisa matematika. Ada tiga teknik kriptanalisis dengan analisis matematika untuk pencarian variabel matriks kunci pada *digital signature* kriptografi Hill *Cipher* yang telah diketahui, yaitu dengan menggunakan persamaan linier, perkalian matriks (Munir, 2006), dan determinan matriks (Azhar., dkk. 2017). Ketiga analisis matematika tersebut berlaku apabila potongan *plaintex*-tnya diketahui atau disebut juga dengan serangan *known plaintext attack*. Berikut adalah contoh implementasi kriptanalisis menggunakan analisis matematika menggunakan persamaan linier, perkalian matriks, dan determinan matriks.

a. Persamaan Linier

Langkah-langkah analisis matematika mengunakan persamaan linier adalah sebagai berikut:

1. Diketahui variabel C, K, dan P sebagai berikut:

C = U B E I N G

P = L I K M I Z

$$K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

2. Ambil empat huruf *ciphertext* dan *plaintext,* konversi kedalam angka.

C = $\begin{bmatrix} U & E \\ B & I \end{bmatrix} = \begin{bmatrix} 20 & 4 \\ 1 & 8 \end{bmatrix}$ P = $\begin{bmatrix} L & K \\ I & M \end{bmatrix} = \begin{bmatrix} 11 & 10 \\ 8 & 12 \end{bmatrix}$

3. Implementasikan kedalam rumus Hill *Cipher* C = K . P

$$\begin{bmatrix} 20 & 4 \\ 1 & 8 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 11 & 10 \\ 8 & 12 \end{bmatrix}$$

20 = 11a + 8b

4 = 10a + 12b

1 = 11c + 8d

8 = 10c + 12d

4. Selanjutnya gunakan subtitusi persamaan pada matriks pada hasil dari C = K . P untuk mengetahui nilai dari masing-masing variabel kunci.

$$\frac{11a + 8b = 20}{10a + 12b = 4} -$$

a – 4b = 16

a = 16 + 4b

10a + 12b = 4

10(16+4b) + 12b = 4

160 + 40b + 12b = 4

160 + 52b = 4

52b = 160 – 4

52b = 156

b = $\frac{156}{26}$mod 26

b = 3

a = 16 + 4b

a = 16 + 4(3)

a = 16 + 12

a = 28 mod 26

a = 2

$$\frac{11c + 8d = 1}{10c + 12d = 8} -$$

c – 4d = -7

c = -7 + 4d

11c + 8d = 1

11(-7+4d) + 8d = 1

-77 + 44d + 8d = 1

-77 + 52d = 1

52d = 1 + 77

52d = 78

d = $\frac{52}{26}$mod 26

d = 2

c = -7 + 4d

c = -7 + 4(2)

c = -7 + 8

c = 1

5. Kunci enkripsi ditemukan. Lakukan *inverse* untuk mengetahui kunci dekripsi.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$$

$$\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}^{-1} = \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix}$$

b. Perkalian Matriks

Langkah-langkah analisis matematika mengunakan perkalian matriks adalah sebagai berikut:

1. Diketahui variabel C, K, dan P sebagai berikut:

C = U B E I N G

P = L I K M I Z

$$K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

2. Ambil empat huruf *ciphertext* dan *plaintext,* konversi kedalam angka.

$$C = \begin{bmatrix} U & E \\ B & I \end{bmatrix} = \begin{bmatrix} 20 & 4 \\ 1 & 8 \end{bmatrix} \qquad P = \begin{bmatrix} L & K \\ I & M \end{bmatrix} = \begin{bmatrix} 11 & 10 \\ 8 & 12 \end{bmatrix}$$

3. Implementasikan kedalam rumus Hill *Cipher* K = C . P^{-1}

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 20 & 4 \\ 1 & 8 \end{bmatrix} . \begin{bmatrix} 1 & 2 \\ 2 & 3 \end{bmatrix} \text{mod } 26$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 28 & 55 \\ 27 & 28 \end{bmatrix} \text{mod } 26$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$$

4. Kunci enkripsi ditemukan. Lakukan *inverse* untuk mengetahui kunci dekripsi.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$$

$$\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}^{-1} = \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix}$$

c. Determinan Matriks

Langkah-langkah analisis matematika mengunakan determinan matriks adalah :

1. Diketahui variabel C, K, dan P sebagai berikut:

C = U B E I N G

P = L I K M I Z

$$K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

2. Ambil empat huruf *ciphertext* dan *plaintext,* konversi kedalam angka

$C = \begin{bmatrix} U & E \\ B & I \end{bmatrix} = \begin{bmatrix} 20 & 4 \\ 1 & 8 \end{bmatrix}$ $P = \begin{bmatrix} L & K \\ I & M \end{bmatrix} = \begin{bmatrix} 11 & 10 \\ 8 & 12 \end{bmatrix}$

3. Implementasikan kedalam rumus Hill *Cipher* C = K . P

$$\begin{bmatrix} 20 & 4 \\ 1 & 8 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 11 & 10 \\ 8 & 12 \end{bmatrix}$$

20 = 11a + 8b

4 = 10a + 12b

1 = 11c + 8d

8 = 10c + 12d

4. Cari determinan tiap variabel kunci (Det b dan Det d tidak ditukar posisinya)

Det $= \begin{bmatrix} 11 & 8 \\ 10 & 12 \end{bmatrix}$ Tukar Posisi $= \begin{bmatrix} 8 & 11 \\ 12 & 10 \end{bmatrix}$ 80 – 132 = -52 mod 26 = 26

Det a $= \begin{bmatrix} 20 & 8 \\ 4 & 12 \end{bmatrix}$ Tukar Posisi $= \begin{bmatrix} 8 & 20 \\ 12 & 4 \end{bmatrix}$ 32 – 240 = -208 mod 26 = 52

Det b $= \begin{bmatrix} 20 & 11 \\ 4 & 10 \end{bmatrix}$ 200 – 44 = 156 mod 26 = 78

Det c $= \begin{bmatrix} 1 & 8 \\ 8 & 12 \end{bmatrix}$ Tukar Posisi $= \begin{bmatrix} 8 & 1 \\ 12 & 8 \end{bmatrix}$ 64 – 12= 52 mod 26 = 26

Det d $= \begin{bmatrix} 1 & 11 \\ 8 & 10 \end{bmatrix}$ 10 – 88 = -78 mod 26 = 52

a $= \frac{Deta}{Det} = \frac{52}{26} = 2$ c $= \frac{Detc}{Det} = \frac{26}{26} = 1$

b $= \frac{Detb}{Det} = \frac{78}{26} = 3$ d $= \frac{Detd}{Det} = \frac{52}{26} = 2$

$$K = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$$

$$K^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}^{-1} = \begin{bmatrix} 2 & -3 \\ -1 & 2 \end{bmatrix}$$

4.3 *Step 3 : Vulnerability Identification* (Identifikasi Kerentanan)

Selanjutnya adalah mengidentifikasi kerentanan terhadap *digital signature* kriptografi Hill *Cipher.* Kerentanan yang akan dianalisa adalah berdasarkan ketersediaan data dan berdasarkan kunci Hill *Cipher* yang akan dipakai dalam proses enkripsi dan dekripsinya.

4.3.1 Berdasarkan Ketersedian Data

Yang dimaksud dengan ketersediaan data adalah banyaknya potongan *plaintext* yang diketahui. Pada *digital signature* kriptografi Hill *Cipher,* serangan berupa analisis matematika tersebut berlaku apabila potongan *plaintext*-nya diketahui sebagian atau disebut juga dengan serangan *known plaintext attack*. Jumlah minimal *plaintext* yang diketahui yaitu empat huruf. Misal diketahui potongan *plaintext* dan *ciphertext* sebagai berikut:

Ciphertext : cvsdgvbcnjsvkjvbdshcvbnkjvvbfvjnhfgwhjbfbsfhsjdfnskjbfhvhfbhjdfgnjhd

Plaintext : bila

Maka dengan hanya mengetahui potongan *plaintext*-nya sebanyak empat huruf, kunci Hill *Cipher* dapat diketahui, sehingga *ciphertext* dapat dipecahkan. Contoh kunci yang didapat dari hasil analisis matematika Hill *Cipher*.

Kunci : $\begin{bmatrix} 24 & 7 \\ 19 & 94 \end{bmatrix}$

Karena kunci Hill Cipher telah ditemukan, *ciphertext* di atas dapat diketahui maknanya, yaitu:

Ciphertext : cvsdgvbcnjsvkjvbdshcvbnkjvvbfvjnhfgwhjbfbsfhsjdfnskjbfhvhfbhjdfgnjhd

Plaintext : bila nanti saatnya telah tiba ku ingin kau menjadi milikku

Dari skema diatas dapat disimpulkan bahwa potongan kata “bila” yang berjumlah empat huruf dapat digunakan untuk mencari mencari kunci Hill Cipher. Inilah yang

dimaksud dengan kerentanan dari ketersedian data, yaitu ketersedian data dari potongan *plaintext*.

4.3.2 Berdasarkan Kunci Hill *Cipher*

Berdasarkan kunci Hill *Cipher* ada tiga hal yang dapat dilakukan untuk mendapatkan *ciphertext* kembali menjadi *plaintext* yaitu :

1. Dengan melakukan pencurian, membeli, bahkan menyuap untuk mendapatkan kunci.
2. Ceroboh dalam implementasinya, seperti *ciphertext* yang dikirim beserta dengan kuncinya.
3. Dengan menggunakan kriptanalisis.

Kriptanalisis dengan menggunakan analisis matematika pada *digital signature* kriptografi Hill *Cipher* dapat dilakukan dengan tiga teknik yaitu persamaan linier, perkalian matriks, dan determinan matriks. Berikut adalah penjelasan dari ketiga teknik tersebut:

a. Persamaan linier

Pada persamaan linier, nilai dari masing-masing variabel matriks kunci dapat diketahui, namun tiap variabel matriks kuncinya memiliki keterkaitan antara satu variabel dengan variabel lainnya. Sehingga nilai dari setiap variabel matriks kunci tersebut tidak dapat diketahui pada waktu yang bersamaan, sehingga proses pencarian nilai pada tiap variabel tersebut tidak dapat dilakukan dalam waktu yang singkat (Azhar., dkk. 2017).

b. Perkalian matriks

Pada perkalian matriks, proses pencarian variabel matriks kunci hanya dapat dilakukan jika matriks yang merepresentasikan *plaintext* memiliki invers. Jika matriks yang merepresentasikan *plaintext* tidak memiliki invers maka pencarian kunci tidak dapat dilakukan (Azhar., dkk. 2017).

c. Determinan matriks

Nilai determinan yang didapatkan dari suatu matriks dapat dioperasikan untuk mencari nilai variabel dari operasi aljabar linier yang telah direpresentasikan kedalam bentuk matriks. Masing-masing variabel tersebut dapat melakukan proses operasi

pembagian secara bersamaan, sehingga waktu yang digunakan untuk pencarian nilai masing-masing variabel dapat dilakukan dalam waktu yang singkat (Azhar., dkk. 2017).

4.4 *Step 4 : Control Analysis* (Analisis Kontrol)

Kontrol yang perlu dilakukan adalah dengan mencegah agar potongan pesan sebisa mungkin tidak ditemukan oleh orang lain yang tidak berhak mengakses pesan tersebut. Tidak hanya potongan pesan, namun kunci yang digunakan untuk enkripsi dan dekripsi perlu dirahasiakan untuk mencegah kebocoran pesan. Tabel 4.1 merupakan gambaran dari kontrol analisis yang sudah dilakukan terhadap kerentanan dari *digital signature* kriptografi Hill *Cipher* yang *vulnerability*-nya sudah dijelaskan pada *step* sebelumnya.

Tabel 4.1
Kontrol Analisis

No	*Vulnerability*	*Control*
1.	Berdasarkan Ketersediaan Data	Kontrol yang dilakukan adalah dengan merahasiakan potongan pesan agar tidak ditemukan oleh orang lain yang tidak berhak mengkases pesan tersebut, terutama rahasiakan dari seseorang yang berpotensi melakukan kriptanalisis. Tidak hanya potongan *plaintext,* namun kunci yang digunakan untuk enkripsi dan dekripsi perlu dirahasiakan.
2.	Berdasarkan Kunci Hill *Cipher*	
a.	Dengan melakukan pencurian, membeli, bahkan menyuap untuk mendapatkan kunci.	Kontrol yang dilakukan adalah dengan menghindari kecerobohan saat mengirim pesan, jangan sampai pesan terkirim beserta dengan kuncinya. Dan untuk si pembuat pesan apabila menggunakan orang ketiga sebagai pengirim pesan, pastikan psikologis si pengirim pesan tidak mudah di bujuk seperti mudah diancam dan mudah disuap.
b.	Ceroboh seperti *ciphertext* yang dikirim beserta dengan kuncinya.	
c.	Menggunakan kriptanalisis.	
	1. Persamaan Linier	Kontrol yang dilakukan untuk mencegah kriptanalisis adalah dengan membuat nilai variabel kunci matriks pertama sulit dicari agar variabel-variabel kunci berikutnya tidak ditemukan.
	2. Perkalian Matriks	Kontrol yang dilakukan untuk mencegah kriptanalisis adalah dengan menggunakan kunci Hill *Cipher* yang determinannya bukan sama dengan satu.
	3. Determinan Matriks	Belum ada kontrol yang dapat mencegah serangan dari analisis matematika dengan teknik determinan matriks. Saat ini teknik kriptanalisis menggunakan determinan matriks sangat rentan untuk Hill *Cipher* yang menggunakan kunci matriks dengan ordo 2x2.

4.5 *Step 5 : Likelihood Determination* (Kemungkinan Penentuan)

Kemungkinan potensi kerentanan sebuah pesan yang sudah ditandatangani oleh *digital signature* kriptografi Hill *Cipher* terhadap *vulnerability*-nya dapat digambarkan dengan tingkat *high, medium,* dan *low*. Tabel 4.2 menggambarkan tingkat definisi kemungkinan berdasarkan kerentanan-kerentanan yang sudah dijelaskan pada *step* sebelumnya serta alasan dari masing-masing kerentanan tersebut dikategorikan *high*, *medium*, dan *low*.

Tabel 4.2
Definisi Kemungkinan

No	*Vulnerability*	*Level*	Definisi Kemungkinan
1.	Berdasarkan Ketersediaan Data	*Low*	Identifikasi kerentanan berdasarkan ketersediaan data dikategorikan kedalam *low risk* karena si pengirim pesan hanya perlu merahasiakan potongan pesan dan kunci Hill *Cipher* tidak diketahui oleh oranglain selain penerima pesan.
2.	Berdasarkan Kunci Hill *Cipher*		
a.	Melakukan pencurian, membeli, bahkan menyuap untuk mendapatkan kunci.	*Medium*	Identifikasi kerentanan dengan melakukan pencurian, membeli, bahkan menyuap untuk mendapatkan kunci dikategorikan kedalam *medium risk* karena si pembuat pesan hanya perlu mengidentifikasi psikolgis si pengirim pesan. Pikologis seseorang dapat diidentifikasi melalui kegiatan sehari-hari serta dapat diketahui melalui tes psikologis.
b.	Ceroboh seperti *ciphertext* yang dikirim beserta dengan kuncinya.	*High*	Identifikasi kerentanan kepada seseorang yang ceroboh seperti *ciphertext* yang dikirim beserta dengan kuncinya dikategorikan kedalam *high risk* karena kecerobohan dapat dilakukan oleh siapa saja secara tidak terduga akibat ketidak berhati-hatian atau akibat kurang fokus meskipun kegiatan tersebut sudah dilakukan berulang. Kecerobohan dapat diminimalisir dengan melakukan persiapan dengan matang
c.	Menggunakan kriptanalisis		
	1. Persamaan Linier	*Low*	Analisis matematika dengan teknik persamaan linier dikategorikan kedalam *low risk* karena tiap variabel matriks kunci memiliki keterkaitan antara satu variabel dengan variabel lainnya. Apabila salah satu variabel kunci tidak ditemukan, maka variabel lain sudah dipastikan tidak dapat dicari nilainya. Selain itu nilai dari setiap variabel matriks kunci tersebut tidak dapat diketahui pada waktu yang bersamaan, sehingga proses pencarian nilai

No	*Vulnerability*	*Level*	Definisi Kemungkinan
			pada tiap variabel tersebut tidak dapat dilakukan dalam waktu yang singkat.
	2. Perkalian Matriks	*Medium*	Analisis matematika dengan teknik perkalian matriks dikategorikan kedalam *medium risk* karena proses pencarian kunci matriks hanya dapat dilakukan jika matriks yang merepresentasikan *plaintext* memiliki invers. Jika matriks yang merepresentasikan *plaintext* tidak memiliki invers maka pencarian kunci tidak dapat dilakukan.
	3. Determinan Matriks	*High*	Analisis matematika dengan teknik determinan matriks dikategorikan kedalam *high risk* karena dengan mengunakan determinan matriks masing-masing variabel kunci matriks Hil *Cipher* dapat ditemukan secara bersamaan. Semua jenis matriks kunci dapat ditemukan walaupun determinan matriks tersebut tidak sama dengan satu.

4.6 *Step 6 : Impact Analysis* (Analisis Dampak)

Dampak yang diakibatkan oleh kerentanan Hill *Cipher* dapat menimbulkan kerugian seperti rusaknya integritas pada pesan, hilangnya kerahasiaan pada pesan, serta hilangnya ketersediaan data pada pesan. Kerusakan pada pesan tersebut tidak dapat diukur secara kuantitatif namun dapat dikualifikasi dalam tingkatan seperti *high, medium,* dan *low* dalam penggambarannya. Berikut adalah dampak akibat ancaman kerentanan terhadap pesan yang sudah ditandatangani dengan *digital signature* kriptografi Hill *Cipher* seperti yang terdapat pada Tabel 4.3.

Tabel 4.3
Besaran Definisi Dampak

Level	Definisi Dampak
High	Kehilangan Integritas. Integritas hilang jika perubahan yang tidak sah dilakukan terhadap data dengan tindakan yang disengaja atau tidak disengaja. Kehilangan integritas dapat mengakibatkan ketidakakuratan, kecurangan, atau keputusan yang keliru. Pelanggaran integritas mungkin merupakan langkah awal dalam serangan melawan kerahasiaan sistem.
Medium	Hilangnya Kerahasiaan. Sistem dan kerahasiaan data mengacu pada perlindungan informasi. Dampak pengungkapan informasi rahasia yang tidak sah, tidak diantisipasi, atau tidak disengaja dapat mengakibatkan hilangnya kepercayaan publik, atau bahkan bisa berdampak pada tindakan hukum.
Low	Kehilangan Ketersediaan Data. Hilangnya fungsionalitas sistem dapat mengakibatkan hilangnya waktu produktif, sehingga menghambat kinerja pengguna dalam mendukung misi organisasi.

4.7 *Step 7 : Risk Determination* (Penentuan Risiko)

Penentuan risiko *digital signature* kriptografi Hill *Cipher* terhadap kerentannya

dapat dilakukan dengan menggunakan matriks tingkat risiko dan deskripsi tingkat risiko.

4.7.1 Matriks Tingkat Risiko

Dalam penelitian ini matriks tingkat risiko yang digunakan adalah matriks dengan ordo 3 x 3, dan variabel tingkatan yang digunakan adalah *high, medium,* dan *low.* Matriks pada Tabel 4.4 menunjukkan tingkat risiko pada definisi kemungkinan-kemungkinan serta dampaknya.

Tabel 4.4
Implementasi Matriks Tingkat Risiko

Threat ***Likelihood***	***Impact***		
	***Low* (10)** **Hilang Ketersediaan Data**	***Medium* (50)** **Hilang Kerahasiaan**	***High* (100)** **Hilang Integritas Data**
***Low* (0.1)** **Ketersediaan Data**	*Low* 10 X 0.1 = 1	*Low* 50 X 0.1 = 5	*Low* 100 X 0.1 = 10
***Medium* (0.5)** **Mencuri, membeli, dan menyuap**	*Low* 10 X 0.5 = 5	*Medium* 50 X 0.5 = 25	*Medium* 100 X 0.5 = 50
***High* (1.0)** **Ceroboh**	*Low* 10 X 1.0 = 10	*Medium* 50 X 1.0 = 50	*High* 100 X 1.0 = 100
***High* (1.0)** **Determinan Matriks**	*Low* 10 X 1.0 = 10	*Medium* 50 X 1.0 = 50	*High* 100 X 1.0 = 100
***Medium* (0.5)** **Perkalian Matriks**	*Low* 10 X 0.5 = 5	*Medium* 50 X 0.5 = 25	*Medium* 100 X 0.5 = 50
***Low* (0.1)** **Persamaan Linier**	*Low* 10 X 0.1 = 1	*Low* 50 X 0.1 = 5	*Low* 100 X 0.1 = 10

4.7.2 Deskripsi Tingkat Risiko

Tabel 4.5 merupakan deskripsi skala risiko dan tindakan yang harus dilakukan berdasarkan tingkatannya. Deskripsi dari tabel tersebut berdasarkan tabel matriks tingkat risiko sebelumnya.

Tabel 4.5
Skala Risiko dan Tindakan yang Diperlukan

Level	Deskripsi Risiko dan Tindakan yang Diperlukan
High	Jika pengamatan dievaluasi sebagai risiko tinggi, ada kebutuhan yang kuat untuk tindakan perbaikan pada sistem *digital signature* kriptografi Hill *Cipher* dan tindakan tersebut harus dilakukan sesegera mungkin.
Medium	Jika pengamatan dinilai sebagai risiko menengah, tindakan perbaikan pada sistem *digital signature* kriptografi Hill *Cipher* perlu direncanakan, dan harus dikembangkan dalam jangka waktu yang wajar.
Low	Jika pengamatan digambarkan sebagai risiko rendah, sistem *digital signature* kriptografi Hill *Cipher* harus menentukan apakah tindakan perbaikan masih

diperlukan atau memutuskan untuk menerima risikonya.

4.8 *Step 8 : Control Recommendations (Rekomendasi Kontrol)*

Pada Tabel 4.6 terdapat kontrol yang akan direkomendasikan yang bertujuan untuk mengurangi tingkat risiko terhadap kerentanan-kerentanan pada pesan yang sudah ditandatangani *digital signature* kriptografi Hill *Cipher* kepada tingkat yang dapat diterima.

Tabel 4.6
Rekomendasi Kontrol

No	*Vulnerability*	*Control Recommendations*
1.	Berdasarkan Ketersediaan Data	Kontrol yang perlu dilakukan adalah merahasiakan potongan pesan dan kunci Hill *Cipher* agar tidak diketahui oleh oranglain selain penerima pesan. Pilih media penyimpanan pesan dan kunci yang aman sebagai langkah utama untuk menghindari kriptanalisis.
2.	Berdasarkan Kunci Hill *Cipher*	
a.	Melakukan pencurian, membeli, bahkan menyuap untuk mendapatkan kunci.	Kontrol yang perlu dilakukan adalah dengan mengidentifikasi psikolgis si pengirim pesan. Pikologis si pengirim pesan dapat diidentifikasi oleh si pembuat pesan melalui kegiatan sehari-hari. Apabila diperlukan lakukan tes psikologis pada si pengirim pesan.
b.	Ceroboh seperti *ciphertext* yang dikirim beserta dengan kuncinya.	Kontrol yang perlu dilakukan adalah dengan melakukan persiapan pengiriman pesan dengan matang seperti pertimbangan pada media penyimpanan pesan, media penyimpanan kunci, dan memperhatikan psikologis si pengirim pesan.
c.	Menggunakan kriptanalisis	
	1. Persamaan Linier	Kontrol yang perlu dilakukan adalah dengan menggunakan teknik yang sama dengan teknik Hill Cipher versi asli, namun teknik yang digunakan dilakukan sebanyak dua kali.
	2. Perkalian Matriks	Kontrol yang perlu dilakukan adalah dengan menambahkan variabel angka 0 - 9 pada tabel definisi Hill *Cipher,* sehingga karakter Hill *Cipher* bertambah dari 26 karakter menjadi 36 karakter.
	3. Determinan Matriks	Kontrol yang perlu dilakukan adalah dengan dengan menggunakan matriks kunci Hill *Cipher* berukuran 3 x 3 untuk proses enkripsi dan dekripsinya.

Berikut adalah contoh penerapan dari teknik rekomendasi kontrol untuk pesan yang akan ditandatangani oleh *digital signature* kriptografi Hill *Cipher* yang mengunakan kriptanalisis analisis matematika dengan teknik persamaan linier, teknik perkalian

matriks, serta teknik determinan matriks:

4.8.1 Mengunakan Hill *Cipher* Sebanyak Dua Kali

Pada bab sebelumnya telah dilakukan proses enkripsi Hill *Cipher* dengan mengunakan *plaintext* “LIKMI” dan hasilnya adalah sebagai berikut:

Plaintext : LIKMI

Ciphertext : UBEING

Kunci : $\begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$

Selanjutnya *ciphertext* yang dihasilkan tersebut diproses kembali menggunakan teknik Hill *Cipher.* Hal ini dilakukan untuk mencegah kriptanalisis dengan analisis matematika dengan teknik persamaan linier. Cara perhitungannya sama dengan teknik Hill *Cipher* sebelumya. Berikut adalah contoh penerapannya:

1. Tabel Definisi Hill *Cipher*

Tabel yang digunakan dalam proses enkripsi kedua yaitu menggunakan tabel definisi yang sama pada saat melakukan enkripsi yang pertama. Tabel definisi Hill *Cipher* dapat dilihat pada tabel 4.6.

Tabel 4.7
Definisi Hill Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

2. Kunci Hill *Cipher*

Langkah selanjutnya adalah menentukan kunci Hill *Cipher* yang akan digunakan pada saat enkripsi kedua. Kunci yang digunakan dapat sama ataupun berbeda dari kunci pada proses enkripsi yang pertama. Dalam penelitian ini penulis menggunakan kunci yang sama dengan proses enkripsi pertama.

$$K = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$$

3. Plaintext

Hal berikutnya yang dilakukan adalah menentukan *plaintext* yang akan dienkripsi. *Plaintext* yang akan digunakan adalah *ciphertext* yang didapat pada saat melakukan proses enkripsi yang pertama, yaitu kata “UBEING”.

$$\begin{bmatrix}U\\B\end{bmatrix}=\begin{bmatrix}20\\1\end{bmatrix} \qquad \begin{bmatrix}N\\G\end{bmatrix}=\begin{bmatrix}13\\6\end{bmatrix}$$

$$\begin{bmatrix}E\\I\end{bmatrix}=\begin{bmatrix}4\\8\end{bmatrix}$$

4. Implementasikan ke dalam rumus Hill *Cipher*

Langkah selanjutnya adalah mengimplementasikan kunci dan *plaintext* kedalam rumus Hill *Cipher* yaitu C = K.P mod 26.

$$\begin{bmatrix}U\\B\end{bmatrix}=\begin{bmatrix}2 & 3\\1 & 2\end{bmatrix}.\begin{bmatrix}20\\1\end{bmatrix}=\begin{bmatrix}43\\22\end{bmatrix}\text{mod 26}=\begin{bmatrix}17\\22\end{bmatrix}=\begin{bmatrix}R\\W\end{bmatrix}$$

$$\begin{bmatrix}E\\I\end{bmatrix}=\begin{bmatrix}2 & 3\\1 & 2\end{bmatrix}.\begin{bmatrix}4\\8\end{bmatrix}=\begin{bmatrix}32\\20\end{bmatrix}\text{mod 26}=\begin{bmatrix}6\\20\end{bmatrix}=\begin{bmatrix}G\\U\end{bmatrix}$$

$$\begin{bmatrix}N\\G\end{bmatrix}=\begin{bmatrix}2 & 3\\1 & 2\end{bmatrix}.\begin{bmatrix}13\\6\end{bmatrix}=\begin{bmatrix}44\\25\end{bmatrix}\text{mod 26}=\begin{bmatrix}17\\25\end{bmatrix}=\begin{bmatrix}R\\Z\end{bmatrix}$$

5. Hasil enkripsi

Kata yang dihasilkan setelah melakukan proses enkripsi di atas adalah kata “RWGURZ”. Perbedaan dari proses enkripsi pertama dan kedua adalah seperti berikut:

Plaintext : LIKMI

Ciphertext 1 : UBEING

Ciphertext 2 : RWGURZ

Enkripsi tersebut dikatakan berhasil karena kata “LIKMI” sudah berubah menjadi “RWGURZ”. Sedangkan untuk proses dekripsinya dilakukan sebanyak dua kali. Teknik yang digunakan untuk dekripsi adalah sama seperti dengan teknik yang sudah dijelaskan pada bab sebelumnya.

4.8.2 Menambahkan Variabel Angka pada Karakter Hill *Cipher*

Pada bab sebelumnya telah dilakukan proses enkripsi Hill *Cipher* dengan mengunakan *plaintext* “LIKMI” yan

g mengunakan tabel definisi sebanyak 26 karakter dan hasilnya sebagai berikut:

Plaintext : LIKMI Kunci : $\begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$

Ciphertext : UBEING

Pada tahap ini tabel defins Hill *Cipher* 26 karakter diganti dengan tabel definisi Hill *Cipher* sebanyak 35 karakter. Hal ini dilakukan untuk mencegah kriptanalisis dengan analisis matematika dengan teknik perkalian matriks. Cara perhitungannya sama dengan teknik Hill *Cipher* sebelumya. Berikut adalah contoh penerapannya:

1. Tabel Definisi Hill *Cipher*

Tabel yang digunakan adalah tabel definisi Hill Cipher sebanyak 36 karakter yaitu dengan menambah variabel angka 0 – 9. Tabel definisi Hill *Cipher* 36 karakter dapat dilihat pada tabel 4.7.

Tabel 4.8
Definisi Hill Cipher 35 Karakter

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35

2. Kunci Hill *Cipher*

Langkah selanjutnya adalah menentukan kunci Hill *Cipher* yang akan digunakan pada saat enkripsi. Dalam penelitian ini penulis menggunakan kunci yang sama dengan proses enkripsi pada bab sebelumnya.

$$K = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$$

3. Plaintext

Hal berikutnya yang dilakukan adalah menentukan *plaintext* yang akan dienkripsi. *Plaintext* yang akan penulis gunakan adalah *plaintext* yang sama pada saat proses enkripsi menggunakan tabel definisi 26 karakter pada bab sebelumnya.

$$\begin{bmatrix} L \\ I \end{bmatrix} = \begin{bmatrix} 11 \\ 8 \end{bmatrix} \qquad \begin{bmatrix} I \\ Z \end{bmatrix} = \begin{bmatrix} 8 \\ 25 \end{bmatrix}$$

$$\begin{bmatrix} K \\ M \end{bmatrix} = \begin{bmatrix} 10 \\ 12 \end{bmatrix}$$

4. Implementasikan ke dalam rumus Hill *Cipher*

Langkah selanjutnya adalah mengimplementasikan kunci dan *plaintext* kedalam rumus Hill *Cipher* yang baru yaitu C = K.P mod 36. Modulus pembagi dalam rumus Hill *Cipher* pada teknik ini berubah menjadi 36 karena tabel definisi yang digunakan adalah 36 karakter.

$$\begin{bmatrix} L \\ I \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} . \begin{bmatrix} 11 \\ 8 \end{bmatrix} = \begin{bmatrix} 46 \\ 27 \end{bmatrix} \text{mod } 36 = \begin{bmatrix} 10 \\ 27 \end{bmatrix} = \begin{bmatrix} K \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} K \\ M \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} . \begin{bmatrix} 10 \\ 12 \end{bmatrix} = \begin{bmatrix} 56 \\ 34 \end{bmatrix} \text{mod } 36 = \begin{bmatrix} 20 \\ 34 \end{bmatrix} = \begin{bmatrix} U \\ 8 \end{bmatrix}$$

$$\begin{bmatrix} I \\ Z \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix} . \begin{bmatrix} 8 \\ 25 \end{bmatrix} = \begin{bmatrix} 91 \\ 58 \end{bmatrix} \text{mod } 36 = \begin{bmatrix} 19 \\ 22 \end{bmatrix} = \begin{bmatrix} T \\ W \end{bmatrix}$$

5. Hasil enkripsi

Kata yang dihasilkan setelah melakukan proses enkripsi di atas adalah kata “K1U8TW”. Perbedaan dari proses enkripsi pertama dan kedua adalah seperti berikut:

Plaintext : LIKMI

Tabel 26 Karakter : UBEING

Tabel 36 Karakter : K1U8TW

Enkripsi tersebut dikatakan berhasil karena kata “LIKMI” sudah berubah menjadi “K1U8TW”. Sedangkan untuk proses dekripsinya adalah sama seperti dengan teknik yang sudah dijelaskan pada bab sebelumnya. Perbedaanya adalah dengan menggunakan pembagian modulus 36 yaitu $P = K^{-1}.C \bmod 36$.

4.8.3 Mengunakan Matriks Kunci Hill *Cipher* Berukuran 3 x 3

Pada bab sebelumnya telah dilakukan proses enkripsi Hill *Cipher* dengan mengunakan *plaintext* “LIKMI” yang mengunakan kunci matriks berukuran 2 x 2 dan hasilnya sebagai berikut:

Plaintext : LIKMI

Ciphertext : UBEING

Kunci : $\begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$

Pada tahap ini kunci matriks Hill *Cipher* yang digunakan bukan berukuran 2 x 2, melainkan berukuran 3 x 3. Hal ini dilakukan untuk mencegah kriptanalisis dengan analisis matematika dengan teknik determinan matriks. Cara perhitungannya sama dengan teknik Hill *Cipher* sebelumya. Berikut adalah contoh penerapannya:

1. Tabel Definisi Hill *Cipher*

Tabel yang digunakan dalam proses enkripsi ini adalah menggunakan tabel definisi yang sama pada saat melakukan enkripsi pada bab sebelumnya. Tabel definisi Hill *Cipher* dapat dilihat pada tabel 4.8.

Tabel 4.9
Definisi Hill Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

2. Kunci Hill *Cipher*

Langkah selanjutnya adalah menentukan kunci Hill *Cipher* yang akan digunakan pada saat enkripsi. Dalam penelitian ini penulis menggunakan kunci yang berbeda dengan proses enkripsi pada bab sebelumnya. Kunci yang digunakan dalam penelitian ini berukuran 3 x 3.

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

3. Plaintext

Berikutnya yang dilakukan adalah menentukan *plaintext* yang akan dienkripsi. *Plaintext* yang akan gunakan adalah *plaintext* yang sama pada saat proses enkripsi pada bab sebelumnya. Dalam penelitian ini plaintext tersebut dibagi menjadi 3 blok matriks.

$$\begin{bmatrix} L \\ I \\ K \end{bmatrix} = \begin{bmatrix} 11 \\ 18 \\ 10 \end{bmatrix} \qquad \begin{bmatrix} M \\ I \\ Z \end{bmatrix} = \begin{bmatrix} 12 \\ 8 \\ 25 \end{bmatrix}$$

4. Implementasikan ke dalam rumus Hill *Cipher*

Langkah selanjutnya adalah mengimplementasikan kunci dan *plaintext* kedalam rumus Hill *Cipher* yang baru yaitu C = K.P mod 26.

$$\begin{bmatrix} L \\ I \\ K \end{bmatrix} = \begin{bmatrix} 17\ 17\ 5 \\ 21\ 18\ 21 \\ 2\ \ 2\ 19 \end{bmatrix} . \begin{bmatrix} 11 \\ 18 \\ 10 \end{bmatrix} = \begin{bmatrix} 543 \\ 765 \\ 248 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 23 \\ 11 \\ 14 \end{bmatrix} = \begin{bmatrix} X \\ L \\ O \end{bmatrix}$$

$$\begin{bmatrix} M \\ I \\ Z \end{bmatrix} = \begin{bmatrix} 17\ 17\ 5 \\ 21\ 18\ 21 \\ 2\ \ 2\ 19 \end{bmatrix} . \begin{bmatrix} 12 \\ 8 \\ 25 \end{bmatrix} = \begin{bmatrix} 465 \\ 921 \\ 515 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 23 \\ 11 \\ 21 \end{bmatrix} = \begin{bmatrix} X \\ L \\ V \end{bmatrix}$$

5. Hasil enkripsi

Kata yang dihasilkan setelah melakukan proses enkripsi di atas adalah kata “XLOXLV”. Perbedaan dari proses enkripsi dengan menggunakan kunci dengan ordo 2 x 2 dan 3 x 3 adalah seperti berikut:

Plaintext : LIKMI

Kunci 2 x 2 : UBEING

Kunci 3 x 3 : XLOXLV

Enkripsi tersebut dikatakan berhasil karena kata “LIKMI” sudah berubah menjadi “XLOXLV”. Sedangkan untuk proses dekripsinya adalah sama seperti dengan teknik yang sudah dijelaskan pada bab sebelumnya. Perbedaanya adalah pembagian blok pada matriks nya adalah tiga pada pada masing-masing matriks.

4.9 *Step 9 : Results Documentation* (Hasil Dokumentasi)

Hasil dari penilaian risiko yang telah dilakukan didokumentasikan dalam bentuk

laporan tesis ini. Laporan penilaian risiko tersebut dapat digunakan untuk menilai risiko terhadap pesan yang sudah ditandatangani oleh *digital signature* kriptografi Hill *Cipher* terhadap kerentan Hill *Cipher* serta upaya pencegahannya, sehingga teknik pencegahan yang akan dilakukan untuk mengurangi dan memperbaiki potensi kerugian dari *digital signature* kriptografi Hill *Cipher* tersebut dapat dilakukan.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan penelitian yang telah dilakukan, maka dapat ditarik kesimpulan sebagai berikut:

1. Teknik *risk assessment* pada *digital signature* kriptografi Hill *Cipher* yang dilakukan dengan menggunakan NIST 800-30 dapat mengurangi dampak akibat kerentanan yang terdapat pada Hill *Cipher*.
2. Upaya *risk assessment* untuk mengurangi dampak akibat kerentanan terhadap pesan yang sudah diotentikasi menggunakan *digital signature* kriptografi Hill *Cipher* dapat dilakukan.

5.2 Saran

Berdasarkan kesimpulan di atas, tentunya masih banyak kekurangan dalam aplikasi yang penulis bangun. Penelitian ini masih dapat dikembangkan lagi untuk ke depannya, seperti:

1. Teknik *risk assessment* pada *digital signature* perlu dikembangkan dalam otentikasi pesan dengan menggunakan *digital signature* dengan teknik kriptografi lain.
2. Teknik rekomendasi kontrol yang diusulkan penulis perlu dikembangkan untuk menghindari risiko terhadap kerentanan Hill *Cipher*.
3. Diperlukan manajemen waktu yang lebih disiplin dan sumber daya manusia yang berkualitas dalam melakukan penelitian untuk kedepannya.

DAFTAR PUSTAKA

Azhar, Wafiqah Yasmin., Supriyadi., Yanitasari, Yessy. 2017. ***"Kriptanalisis Hill Cipher Terhadap Known Plaintext Attack Menggunakan Metode Determinan Matriks Berbasis Android"***. Jurnal SIMETRIS, Vol 8 No 2. Teknik Informatika STMIK Kharisma Karawang.

Cahyono, Murti. 2014. "***Implementasi Algoritma Hill Cipher Pada Aplikasi Sms Berbasis Android".*** Teknik Informatika Amikom Yogyakarta, Yogyakarta.

Kromodimoeljo, Sentot. 2009. ***Teori dan Aplikasi Kriptografi***. SPK IT Consulting.

Menezes, Alfred., Oorschot, Paul C. van., Vanstone, Scott. 1996. ***"Handbook of Applied Cryptography"***. Massachusetts Institute of Technology. Boston, USA.

Munir, Rinaldi. 2004. ***"Otentikasi dan Tandatangan Digital".*** IF5054 Kriptografi. Departemen Teknik Informatika. Institut Teknologi Bandung.

Munir, Rinaldi. 2006. "***Kriptografi"***. Informatika, Bandung.

[NA : Network Associates, Inc]. US. 1999. ***"An Introduction to Cryptography".*** Santa Clara. United States of America.

Paar , Christof., Pelzl, Jan. 1998. ***"Understanding Cryptography"***. Springer Heidelberg Dordrecht. London, New York.

Santosa. Edgar Dika. 2015. "***Implementasi Algoritma Caesar Cipher Dan Hill Cipher Pada Database Sistem Inventori Tb Mita Jepara".*** Teknik Informatika Universitas Dian Nuswantoro, Semarang.

Schaefer, Edward. 2010. ***"An Introduction to Cryptography and Cryptanalysis"***. Santa Clara University, United States of America.

Stallings, William. 1995. ***"Network and Internetwork Security".*** Prentice Hall. The Institute of Electrical and Electronics Engineer, Inc., New York.

Stoneburner, Gary., Goguen, Alice., Feringa, Alexis. 2002. ***"Risk Management Guide for Information Technology Systems".*** NIST 800-30. Computer Security Division Information Technology Laboratory.

Worthington, Brian. 2010. "***An Introduction to Hill Ciphers Using Linear Algebra".*** University of North Texas.